IPv6 コマンド リファレンス、Cisco IOS XE Release 3SE（Catalyst 3850 スイッチ）

初版：2013 年 01 月 11 日

最終更新：2013 年 01 月 22 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

ipv6-a1 1

- allow 2
- clear bgp ipv6 4
- clear ipv6 mtu 8
- default-metric（OSPFv3） 9
- deny（IPv6） 11
- destination-glean 22
- device-role 24
- drop-unsecure 26
- enforcement 28
- graceful-restart 30
- hop-limit 32
- interval-option 34
- ipv6 access-list 35
- ipv6 address 40
- ipv6 address anycast 43
- ipv6 address autoconfig 45
- ipv6 address dhcp 47
- ipv6 address eui-64 49
- ipv6 address link-local 52
- ipv6 cef 55
- ipv6 cef accounting 58
- ipv6 cef distributed 61

ipv6-i1 63

- ipv6 dhcp guard attach-policy 65
- ipv6 dhcp guard policy 67
- ipv6 dhcp ping packets 69
- ipv6 dhcp server 71
- ipv6 enable 74

ipv6 host 76
ipv6 icmp error-interval 78
ipv6 nd cache expire 81
ipv6 nd inspection 83
ipv6 nd inspection policy 85
ipv6 nd na glean 87
ipv6 nd nud retry 88
ipv6 nd ra-throttle attach-policy 90
ipv6 nd ra-throttle policy 92
ipv6 nd raguard attach-policy 94
ipv6 nd raguard policy 96
ipv6 nd router-preference 98
ipv6 nd suppress attach-policy 100
ipv6 nd suppress policy 102
ipv6 neighbor binding logging 104
ipv6 neighbor binding max-entries 106
ipv6 neighbor binding vlan 108
ipv6 neighbor tracking 110
ipv6 prefix-list 112
ipv6-i4 117
ipv6 snooping attach-policy 119
ipv6 snooping policy 121
ipv6 traffic-filter 123
ipv6 verify unicast source reachable-via 125
managed-config-flag 128
match ipv6 130
match ipv6 access-list 133
match ipv6 address 135
match ipv6 destination 139
match ipv6 hop-limit 142
match ra prefix-list 144
max-through 146
medium-type 147
mode dad-proxy 148
network（IPv6） 150

other-config-flag 152
passive-interface（IPv6） 154
passive-interface（OSPFv3） 156
permit（IPv6） 158
prefix-glean 171
protocol（IPv6） 173
redistribute（IPv6） 175
router-preference maximum 182
ipv6-r1 185
sec-level minimum 187
server name（IPv6 TACACS+） 189
show ipv6 access-list 191
show ipv6 dhcp conflict 195
show ipv6 interface 197
show ipv6 mld snooping 207
show ipv6 nd ra-throttle policy 209
show ipv6 nd ra-throttle vlan 210
show ipv6 nd raguard policy 211
show ipv6 neighbor binding 213
show ipv6 neighbors 215
show ipv6 protocols 222
show ipv6 route 227
show ipv6 snooping capture-policy 233
show ipv6 snooping counters 235
show ipv6 snooping features 237
show ipv6 snooping policies 239
show ipv6 traffic 241
summary-prefix（OSPFv3） 245
throttle-period 248
timers spf（IPv6） 249
timers throttle lsa 251
tracking 253
tunnel mode ipv6ip 256
vlan configuration 262

ipv6-a1

- allow, 2 ページ
- clear bgp ipv6, 4 ページ
- clear ipv6 mtu, 8 ページ
- default-metric（OSPFv3）, 9 ページ
- deny（IPv6）, 11 ページ
- destination-glean, 22 ページ
- device-role, 24 ページ
- drop-unsecure, 26 ページ
- enforcement, 28 ページ
- graceful-restart, 30 ページ
- hop-limit, 32 ページ
- interval-option, 34 ページ
- ipv6 access-list, 35 ページ
- ipv6 address, 40 ページ
- ipv6 address anycast, 43 ページ
- ipv6 address autoconfig, 45 ページ
- ipv6 address dhcp, 47 ページ
- ipv6 address eui-64, 49 ページ
- ipv6 address link-local, 52 ページ
- ipv6 cef, 55 ページ
- ipv6 cef accounting, 58 ページ
- ipv6 cef distributed, 61 ページ

allow

RA スロットル ポリシーのスロットル期間ごとのデバイスあたりのマルチキャスト ルータ アドバタイズメント（RA）数を制限するには、IPv6 RA スロットル ポリシー コンフィギュレーション モードで **allow** コマンドを使用します。 コマンドをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

allow {**at-least** | {*al-value*| **no-limit**}} | {**at-most** | {*am-value*| **no-limit**}} | {**inherited**}

構文の説明

at-least	スロットリング前にデバイスから受け入れるマルチキャストRAの最小数。
al-value	at-least の値。 • 0 ～ 32 の整数を指定できます。
no-limit	RA スロットリングは発生しません。
at-most	スロットリング前にデバイスから受け入れるマルチキャストRAの最大数。
am-value	at-most の値。 • 0 ～ 256 の整数を指定できます。
inherited	ターゲット ポリシー間の設定を継承または結合します。

コマンド デフォルト

at-least 値は 1 です。

at-most 値は 1 です。

コマンド モード

IPv6 RA スロットル ポリシー コンフィギュレーション モード（config-nd-ra-throttle）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

VLAN レベルで適用される **allow at-least** および **allow at-most** コマンド設定は、VLAN 内のすべてのデバイスのデフォルトを指定します。 RA を発行したデバイスが **allow at-least** コマンド設定によって設定されている RA 数を送信しなかった場合、RA はすべてのホストにマルチキャスト送信されます。 RA を発行したデバイスが **allow at-most** コマンド設定によって設定されている RA 数を送信している場合、RA はスロットリングされます。つまり、RA はすべての有線ホストと、保留中のルータ送信要求（RS）がある無線ホストにマルチキャスト送信されます。

allow at-least と **allow at-most** の値の設定が、すべてのポートのすべてのデバイスで同じ場合、その VLAN にポリシーを適用するだけで済みます。 有線ポートの一部が接続ワイヤレス アクセス ポイントである場合、これらのポートに適用する必要があるのは、設定するメディア タイプのポリシーだけです。

例

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# allow at-least 2 at-most 2
```

clear bgp ipv6

IPv6 ボーダー ゲートウェイ プロトコル（BGP）セッションをリセットするには、特権 EXEC モードで **clear bgp ipv6** コマンドを使用します。

[1]

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。
multicast	IPv6 マルチキャスト アドレス プレフィックスを指定します。
*	現在のすべての BGP セッションをリセットします。
autonomous-system-number	指定された自律システム内の BGP ネイバーの BGP セッションをリセットします。
ip-address	指定した IPv4 BGP ネイバーへの TCP 接続をリセットし、BGP テーブルからの接続から学習したすべてのルートを除外します。
ipv6-address	指定した IPv6 BGP ネイバーへの TCP 接続をリセットし、BGP テーブルからの接続から学習したすべてのルートを除外します。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
peer-group-name	指定した IPv6 BGP ネイバーへの TCP 接続をリセットし、BGP テーブルからの接続から学習したすべてのルートを除外します。
soft	（任意）ソフトリセットを行います。セッションはリセットしないでください。

1

in **out**	（任意）インバウンドまたはアウトバウンドソフト再設定を開始します。 オプション **in** または **out** が指定されていない場合、インバウンドソフトリセットとアウトバウンドソフトリセットの両方がトリガーされます。

コマンド デフォルト リセットは開始されません。

コマンド モード 特権 EXEC

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.3(2)T	**unicast** キーワードが、Cisco IOS Release 12.3(2)T で追加されました。
12.0(26)S	**unicast** および **multicast** キーワードが、Cisco IOS Release 12.0(26)S で追加されました。
12.3(4)T	**multicast** キーワードが、Cisco IOS Release 12.3(4)T で追加されました。
12.2(25)S	**multicast** キーワードが、Cisco IOS Release 12.2(25)S で追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ ルータで追加されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI に統合されました。

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

clear bgp ipv6 コマンドは **clear ip bgp** コマンドと類似していますが、これは IPv6 専用です。

clear bgp ipv6 コマンドを使用すると、指定されたキーワードと引数に応じた重大度レベルでネイバー セッションをリセットできます。

IPv6ユニキャストアドレスプレフィックスでネイバーセッションをドロップするには、**clear bgp ipv6 unicast** コマンドを使用します。

unicast キーワードは、Cisco IOS Release 12.3(2)T 以降のリリースで使用できます。 12.3(2)T よりも前のリリースでは使用できません。 **unicast** キーワードの使用は、Cisco IOS Release 12.3(2)T から必須です。

multicast キーワードは、Cisco IOS Release 12.0(26)S 以降のリリースで利用できます。 12.0(26)S よりも前のリリースでは使用できません。 **unicast** または **multicast** キーワードの使用は、Cisco IOS Release 12.0(26)S から必須です。

全ネイバー セッションをドロップするには、**clear bgp ipv6 *** コマンドを使用します。 Cisco IOS ソフトウェアは、ネイバー接続をリセットします。 この形式のコマンドは次の場合に使用してください。

- BGP タイマーの変更
- BGP アドミニストレーティブ ディスタンスの変更

アウトバウンド ネイバー接続だけをドロップするには、**clear bgp ipv6 soft out** または **clear bgp ipv6 unicast soft out** コマンドを使用します。 インバウンド ネイバー セッションはリセットされません。 この形式のコマンドは次の場合に使用してください。

- BGP 関連のアクセス リストの変更または追加の取得
- BGP 関連の重みの変更
- BGP 関連の配布リストの変更
- BGP 関連のルート マップの変更

インバウンド ネイバー接続だけをドロップするには、**clear bgp ipv6 soft in** または **clear bgp ipv6 unicast soft in** コマンドを使用します。 アウトバウンド ネイバー セッションはリセットされません。 ネイバーのインバウンド ルーティング テーブル アップデートを動的にリセットするには、ルータ リフレッシュ機能をサポートするようにネイバーを設定します。 BGP ネイバーがこの機能をサポートしているかどうかを判断するには、**show bgp ipv6 neighbors** または **show bgp ipv6 unicast neighbors** コマンドを使用します。 ネイバーがルータ リフレッシュ機能をサポートしている場合は、次のメッセージが表示されます。

```
Received route refresh capability from peer.
```

すべてのBGPネットワーク デバイスがルート リフレッシュ機能をサポートしている場合は、**clear bgp ipv6** {*****| ip-*address*| *ipv6-address*| *peer-group-name*} **in** または **clear bgp ipv6 unicast**{*****| ip-*address*| *ipv6-address*| *peer-group-name*} **in** コマンドを使用します。 ソフトウェアが自動的にソフト リセットを実行するため、**soft** キーワードの使用は、ルート リフレッシュ機能がすべての BGP ネットワーク デバイスによってサポートされている場合は必要ではありません。

この形式のコマンドは次の場合に使用してください。

- BGP 関連のアクセス リストの変更または追加の取得
- BGP 関連の重みの変更
- BGP 関連の配布リストの変更
- BGP 関連のルート マップの変更

例

次に、アウトバウンドセッションをリセットせずに、ネイバーが7000::2であるインバウンドセッションをクリアする例を示します。

```
Router# clear bgp ipv6 unicast 7000::2 soft in
```

次に、アウトバウンドセッションをリセットせずに、**unicast**キーワードを使用して、ネイバーが7000::2 であるインバウンド セッションをクリアする例を示します。

```
Router# clear bgp ipv6 unicast 7000::2 soft in
```

次に、インバウンド セッションをリセットせずに、marketing という名前のピア グループを持つアウトバウンド セッションをクリアする例を示します。

```
Router# clear bgp ipv6 unicast marketing soft out
```

次に、インバウンド セッションをリセットせずに、**unicast** キーワードを使用して、peer-group marketing という名前のピア グループを持つアウトバウンド セッションをクリアする例を示します。

```
Router# clear bgp ipv6 unicast peer-group marketing soft out
```

関連コマンド

コマンド	説明
show bgp ipv6	IPv6 BGP ルーティング テーブルのエントリを表示します。

clear ipv6 mtu

メッセージの最大伝送単位（MTU）キャッシュを削除するには、特権 EXEC モードで **clear ipv6 mtu** コマンドを使用します。

clear ipv6 mtu

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

メッセージは MTU キャッシュから削除されません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.6	このコマンドが導入されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ルータが ICMPv6 toobig メッセージでフラッドした場合、ルータはすべての使用可能なメモリが消費されるまで、MTU キャッシュに無制限にエントリを作成します。 MTU キャッシュからメッセージをクリアするには、**clear ipv6 mtu** コマンドを使用します。

例

次の例では、メッセージの MTU キャッシュをクリアします。

```
Router# clear ipv6 mtu
```

関連コマンド

コマンド	説明
ipv6 flowset	ルータが送信する 1280 バイト以上のパケットにフロー ラベル マーキングを設定します。

default-metric（OSPFv3）

Open Shortest Path First バージョン 3（OSPF）ルーティング プロトコルに再配布される IPv4 および IPv6 ルートのデフォルト メトリック値を設定するには、OSPFv3 ルータ コンフィギュレーション モード、IPv6 アドレス ファミリ コンフィギュレーション モード、または IPv4 アドレス ファミリ コンフィギュレーション モードで **default-metric** コマンドを使用します。 デフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

default-metric *metric-value*

no default-metric *metric-value*

構文の説明

metric-value	指定されたルーティング プロトコルに適したデフォルト メトリック値。 指定できる範囲は 1 ～ 4294967295 です。

コマンド デフォルト

各ルーティング プロトコルに適した、組み込みの自動的なメトリック変換。

コマンド モード

OSPFv3 ルータ コンフィギュレーション モード（config-router）

IPv6 アドレス ファミリ コンフィギュレーション（config-router-af）

IPv4 アドレス ファミリ コンフィギュレーション（config-router-af）

コマンド履歴

リリース	変更内容
12.2(15)T	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
15.1(3)S	このコマンドが変更されました。 機能は、IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
Cisco IOS XE Release 3.4S	このコマンドが変更されました。 機能は、IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
15.2(1)T	このコマンドが変更されました。 機能は、IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

default-metric コマンドと **redistribute** ルータ コンフィギュレーション コマンドを組み合わせて使用すると、現在のルーティング プロトコルで、すべての再配布ルートで同じメトリック値が使用されます。 デフォルトのメトリックは、互換性のないメトリックを持つルートを再配布するという問題を解決するために役立ちます。メトリックを変換しない場合、デフォルトメトリックの使用は妥当な代替手段で、再配布が可能となります。

redistribute コマンドのオプションを使用して、再配布されるルートのメトリックを細かく制御できます。

例

次に、IPv6 AF を入力し、process1 という OSPFv3 プロセスからルートを再配布する OSPFv3 ルーティング プロトコルを設定する例を示します。 再配布されるすべてのルートは 10 のメトリックでアドバタイズされます。

```
router ospfv3 100
 address-family ipv6 unicast
 default-metric 10
 redistribute ospfv3 process1
```

次に、process1 という OSPFv3 プロセスからルートを再配布する OSPFv3 ルーティング プロトコルを設定する例を示します。 再配布されるすべてのルートは 10 のメトリックでアドバタイズされます。

```
ipv6 router ospf 100
 default-metric 10
 redistribute ospfv3 process1
```

関連コマンド

コマンド	説明
redistribute（OSPFv3）	あるルーティング ドメインから別のルーティング ドメインへ IPv6 ルートを再配布します。
router ospfv3	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。

deny（IPv6）

IPv6 アクセス リストの拒否条件を設定するには、IPv6 アクセス リスト コンフィギュレーション モードで **deny** コマンドを使用します。 拒否条件を削除するには、このコマンドの **no** 形式を使用します。

deny *protocol* {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] **[undetermined-transport]**

no deny *protocol* {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] **[undetermined-transport]**

Internet Control Message Protocol

deny icmp {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*]| *icmp-message*] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Transmission Control Protocol

deny tcp {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] **[ack]** [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] **[established] [fin]** [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] [**neq** {*port*| *protocol*}] **[psh]** [**range** {*port*| *protocol*}] **[routing]** [**routing-type** *routing-number*] **[rst]** [**sequence** *value*] **[syn]** [**time-range** *name*] **[urg]**

User Datagram Protocol

deny udp {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] [**neq** {*port*| *protocol*}] [**range** {*port*| *protocol*}] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

構文の説明

protocol	インターネットプロトコルの名前または番号。これは、キーワード **ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**sctp**、**tcp**、**udp**、または **hbh** にするか、IPv6 プロトコル番号を表す 0 ～ 255 の整数にすることができます。
source-ipv6-prefix/prefix-length	拒否条件を設定する送信元 IPv6 ネットワークまたはネットワークのクラス。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
any	IPv6 プレフィックス ::/0 の省略形。
host *source-ipv6-address*	拒否条件を設定する送信元 IPv6 ホスト アドレス。 この *source-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。

operator [*port-number*]	（任意）指定のプロトコルの送信元または宛先ポートを比較するオペランドを指定します。オペランドには、**lt**（less than：より小さい）、**gt**（greater than：より大きい）、**eq**（equal：等しい）、**neq**（not equal：等しくない）、および **range**（inclusive range：包含範囲）があります。 *source-ipv6-prefix*/*prefix-length* 引数の後ろに演算子が置かれた場合、送信元ポートと一致する必要があります。 *destination-ipv6*/*prefix-length* 引数の後ろに演算子が置かれた場合、宛先ポートと一致する必要があります。 **range** 演算子には 2 つのポート番号が必要です。他のすべての演算子は 1 つのポート番号が必要です。 任意の *port-number* 引数は 10 進数、または TCP あるいは UDP ポートの名前です。 ポート番号の範囲は 0 ～ 65535 です。 TCP ポート名は TCP をフィルタリングする場合に限り使用できます。 UDP ポート名は UDP をフィルタリングする場合に限り使用できます。
destination-ipv6-prefix/*prefix-length*	拒否条件を設定する宛先 IPv6 ネットワークまたはネットワークのクラス。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
host *destination-ipv6-address*	拒否条件を設定する宛先 IPv6 ホストアドレス。 この *destination-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
auth	任意のプロトコルと組み合わせて、認証ヘッダーのプレゼンスとトラフィックを照合できます。
dest-option-type	（任意）各 IPv6 パケット ヘッダー内のホップバイホップ オプション拡張ヘッダーと IPv6 パケットを照合します。

doh-number	（任意）IPv6宛先オプション拡張ヘッダーを表す 0 から 255 の範囲の整数。
doh-type	（任意）宛先オプション ヘッダー タイプ。 可能な宛先オプション ヘッダー タイプおよび対応する *doh-number* 値は、home-address と 201 です。
dscp *value*	（任意）各IPv6パケットヘッダーのトラフィック クラス フィールドのトラフィック クラス値と DiffServ コード ポイント値を照合します。 指定できる範囲は 0 ～ 63 です。
flow-label *value*	（任意）各 IPv6 パケット ヘッダーのフロー ラベル フィールドのフロー ラベルの値とフロー ラベルの値を照合します。 指定できる範囲は 0 ～ 1048575 です。
fragments	（任意）フラグメント拡張ヘッダーに 0 以外のフラグメント オフセットが含まれる場合、非初期フラグメント パケットを照合します。 **fragments** キーワードは、*operator* [*port-number*] 引数が指定されていない場合に限り指定できるオプションです。
hbh	（任意）ホップバイホップ オプション ヘッダーを指定します。
log	（任意）コンソールに送信されるエントリに一致するパケットに関するロギング メッセージ情報が出力されます。 コンソールにロギングするメッセージのレベルは、**logging console** コマンドで制御します。 メッセージには、アクセス リスト名、シーケンス番号、パケットが拒否されたかどうか、プロトコル（TCP、UDP、ICMP または番号のいずれか）、適正な場合には送信元/宛先アドレス、送信元/宛先ポート番号が含まれます。 メッセージは、一致した最初のパケットに対して生成され、その後、5 分間隔で拒否されたパケット数を含めて生成されます。
log-input	（任意）ロギング メッセージに入力インターフェイスも含まれることを除き、**log** キーワードと同じ機能を提供します。

mobility	（任意）拡張ヘッダーのタイプ。ヘッダー内のモビリティ ヘッダーのタイプ フィールドの値に関係なくモビリティ ヘッダーを含むすべてのIPv6 パケットを照合できます。
mobility-type	（任意）モビリティ ヘッダー タイプ。このキーワードと共に、*mh-number* または *mh-type* 引数を使用する必要があります。
mh-number	（任意）IPv6 モビリティ ヘッダー タイプを表す 0 から 255 の範囲の整数。
mh-type	（任意）モビリティ ヘッダー タイプの名前。次のようなモビリティ ヘッダー タイプと対応する *mh-number* 値が可能です。 • 0：bind-refresh • 1：hoti • 2：coti • 3：hot • 4：cot • 5：bind-update • 6：bind-acknowledgment • 7：bind-error
routing	（任意）ソースルート パケットを、各 IPv6 パケット ヘッダー内の拡張ヘッダーに一致させます。
routing-type	（任意）タイプ フィールドの値を持つルーティング ヘッダーを個別に照合できます。 このキーワードと共に、*routing-number* 引数を使用する必要があります。
routing-number	IPv6 ルーティング ヘッダー タイプを表す 0 から 255 の範囲の整数。 次のようなルーティング ヘッダー タイプと対応する *routing-number* 値が可能です。 • 0：標準 IPv6 ルーティング ヘッダー • 2：モバイル IPv6 ルーティング ヘッダー

sequence *value*	（任意）アクセスリストステートメントのシーケンス番号を指定します。 指定できる範囲は 1 ～ 4294967295 です。
time-range *name*	（任意）拒否ステートメントに適用する時間範囲を指定します。 時間範囲の名前と制限事項は、**time-range** コマンドと、**absolute** または **periodic** コマンドによってそれぞれ指定します。
undetermined-transport	（任意）レイヤ 4 プロトコルを判定できない送信元からのパケットに一致します。 **undetermined-transport** キーワードは、*operator* [*port-number*] 引数が指定されていない場合にのみ任意です。
icmp-type	（任意）ICMP パケットのフィルタリングに ICMP メッセージ タイプを指定します。 ICMP パケットは、ICMP メッセージ タイプでフィルタリングできます。 ICMP メッセージ タイプは、0 ～ 255 の数字で、次のような事前定義された文字列とそれに対応する数値が含まれています。 • 144：dhaad-request • 145：dhaad-reply • 146：mpd-solicitation • 147：mpd-advertisement
icmp-code	（任意）ICMP パケットのフィルタリングに ICMP メッセージ コードを指定します。 ICMP メッセージタイプによってフィルタリングされる ICMP パケットは、ICMP メッセージ コードによってもフィルタリングできます。 メッセージ コードの番号は 0 ～ 255 です。
icmp-message	（任意）ICMP パケットのフィルタリングに ICMP メッセージ名を指定します。 ICMP パケットは、ICMP メッセージ名、または ICMP メッセージタイプおよびコードによってフィルタリングできます。 使用可能な名前については、「使用上のガイドライン」を参照してください。

ack	（任意）TCPプロトコルの場合に限りACKビットを設定します。
established	（任意）TCPプロトコルの場合にだけ、確立された接続を表示します。 TCP データグラムにACKまたはRSTビットが設定されている場合、照合が行われます。 接続するための初期 TCP データグラムの場合は照合しません。
fin	（任意）TCP プロトコルの場合に限り、FIN ビットを設定します。送信元からのデータはこれ以上ありません。
neq {*port* | *protocol*}	（任意）指定のポート番号上にないパケットだけを照合します。
psh	（任意）TCPプロトコルの場合に限りPSHビットを設定します。
range {*port* | *protocol*}	（任意）ポート番号範囲のパケットだけを照合します。
rst	（任意）TCPプロトコルの場合に限りRSTビットを設定します。
syn	（任意）TCPプロトコルの場合に限りSYNビットを設定します。
urg	（任意）TCPプロトコルの場合に限りURGビットを設定します。

コマンド デフォルト

IPv6 アクセス リストは定義されていません。

コマンド モード

IPv6 アクセス リスト コンフィギュレーション (config-ipv6-acl)#

コマンド履歴

リリース	変更内容
12.0(23)S	このコマンドが導入されました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。

リリース	変更内容
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.4(2)T	*icmp-type* 引数が拡張されました。 **dest-option-type**、**mobility**、**mobility-type** および **routing-type** キーワードが追加されました。*doh-number*、*doh-type*、*mh-number*、*mh-type* および *routing-number* 引数が追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 アグリゲーション シリーズ ルータに追加されました。
12.4(20)T	**auth** キーワードが追加されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
15.2(3)T	このコマンドが変更されました。 **hbh** キーワードのサポートが追加されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

deny（IPv6）コマンドは、IPv6 に固有のものを除き、**deny**（IP）コマンドと類似しています。

ipv6 access-list コマンドに続いて、**deny**（IPv6）コマンドを使用すると、パケットがアクセス リストを通過する条件を定義すること、または再帰アクセスリストとしてアクセスリストを定義することができます。

protocol 引数に IPv6 を指定すると、パケットの IPv6 ヘッダーに対して照合を行います。

デフォルトでは、アクセス リストの最初のステートメントの番号は 10 で、その次のステートメントからは 10 ずつ増加します。

permit、**deny**、**remark**、または **evaluate** ステートメントを、リスト全体を再入力せずに既存のアクセスリストに追加できます。新しいステートメントをリストの最後尾以外に追加するには、所属先を示すために 2 つの既存のエントリ番号の間にある適切なエントリ番号を持つ新しいステートメントを作成します。

Cisco IOS Release 12.2(2)T 以降のリリース、12.0(21)ST、および 12.0(22)S では、IPv6 アクセス コントロール リスト（ACL）の定義、および拒否条件と許可条件の設定は、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドと **deny** および **permit** キーワードを使用して行います。 Cisco IOS Release 12.0(23)S 以降のリリースでは、IPv6 ACL は、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用することにより定義され、許可条件と拒否条件は、IPv6 アクセスリスト コンフィギュレーション モードで **deny** コマンドおよび **permit** コマンドを使用して設定されます。 IPv6 ACL の定義の詳細については、**ipv6 access-list** コマンドを参照してください。

（注） Cisco IOS Release 12.0(23)S 以降のリリースでは、IPv6 ACL に最後の一致条件として暗黙の **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および**deny ipv6 any any** ステートメントがあります。（前の 2 つの一致条件により ICMPv6 ネイバー探索が可能になります）。IPv6 ACL には、暗黙の **deny ipv6 any any** ステートメントを有効にするために少なくとも 1 つのエントリが含まれる必要があります。 IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを利用するため、デフォルトで、インターフェイス上での IPv6 ネイバー探索パケットの送受信が IPv6 ACL によって暗黙的に許可されます。 IPv4 の場合、IPv6 ネイバー探索プロセスに相当するアドレス解決プロトコル（ARP）では、個別のデータ リンク層プロトコルを利用するため、デフォルトで、インターフェイス上での ARP パケットの送受信が IPv4 ACL によって暗黙的に許可されます。

source-ipv6-prefix/*prefix-length* と *destination-ipv6-prefix*/*prefix-length* の両方の引数をトラフィックのフィルタリングに使用します（送信元プレフィックスはトラフィックの送信元に基づいて、宛先プレフィックスはトラフィックの宛先に基づいてトラフィックをフィルタリングします）。

（注） アクセス リストでなく、IPv6 プレフィックス リストは、ルーティング プロトコル プレフィックスのフィルタリングに使用する必要があります。

fragments キーワードは、*operator* [*port-number*] 引数が指定されていない場合に限り指定できるオプションです。

undetermined-transport キーワードは、*operator* [*port-number*] 引数が指定されていない場合にのみ任意です。

次に、ICMP メッセージの名前のリストを示します。

- beyond-scope
- destination-unreachable
- echo-reply
- echo-request
- header
- hop-limit
- mld-query

- mld-reduction
- mld-report
- nd-na
- nd-ns
- next-header
- no-admin
- no-route
- packet-too-big
- parameter-option
- parameter-problem
- port-unreachable
- reassembly-timeout
- renum-command
- renum-result
- renum-seq-number
- router-advertisement
- router-renumbering
- router-solicitation
- time-exceeded
- unreachable

例

次に、toCISCO という名前の IPv6 アクセス リストを設定し、イーサネット インターフェイス 0 上の発信トラフィックにアクセスリストを適用する例を示します。具体的には、リストの最初の拒否エントリは、宛先 TCP ポート番号が 5000 よりも大きいすべてのパケットが、イーサネット インターフェイス 0 から出て行かないようにします。 リストの 2 番めの拒否エントリは、送信元 UDP ポート番号が 5000 より小さいすべてのパケットが、イーサネット インターフェイス 0 から出て行かないようにします。 また、この 2 番めの拒否エントリは、すべての一致をコンソールに表示します。 リスト内の最初の許可エントリは、イーサネットインターフェイス 0 から出るすべての ICMP パケットを許可します。 リスト内の 2 番めの許可エントリは、イーサネット インターフェイス 0 から出るその他すべてのトラフィックを許可します。 2 番目の許可エントリは、すべての条件の暗黙的な拒否は各 IPv6 アクセス リストの最後にあるという理由で必要です。

```
ipv6 access-list toCISCO
 deny tcp any any gt 5000
 deny ::/0 lt 5000 ::/0 log
 permit icmp any any
 permit any any
interface ethernet 0
 ipv6 traffic-filter toCISCO out
```

次に、IPsec AH がある場合でも、TCP または UDP の解析を許可する例を示します。

```
IPv6 access list example1
    deny tcp host 2001::1 any log sequence 5
    permit tcp any any auth sequence 10
    permit udp any any auth sequence 20
```

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ipv6 traffic-filter	インターフェイス上の着信または発信 IPv6 トラフィックをフィルタリングします。
permit（IPv6）	IPv6アクセスリストに許可条件を設定します。
show ipv6 access-list	現在のすべての IPv6 アクセス リストの内容を表示します。

destination-glean

宛先アドレス グリーニングによる IPv6 第 1 ホップ セキュリティ バインディング テーブルのリカバリをイネーブルにする、またはリカバリ後に認識されないバインディングテーブルエントリに関する syslog メッセージを生成するには、IPv6 スヌーピング コンフィギュレーション モードで **destination-glean** コマンドを使用します。バインディングテーブルのリカバリを無効にするには、このコマンドの **no** 形式を使用します。

destination-glean {**recovery** | **log-only**} [**dhcp**]

no destination-glean

構文の説明

recovery	宛先アドレス グリーニングによるバインディングテーブルのリカバリをイネーブルにします。
log-only	リカバリ後に認識されないバインディングテーブルエントリに関する syslog メッセージを生成します。
dhcp	宛先アドレスを Dynamic Host Configuration Protocol（DHCP）からリカバリする必要があることを指定します。

コマンド デフォルト

宛先アドレス グリーニングによる IPv6 第 1 ホップ セキュリティ バインディング テーブルのリカバリはイネーブルになりません。

コマンド モード

IPv6 スヌーピング コンフィギュレーション モード（config-ipv6-snooping）

コマンド履歴

リリース	変更内容
15.2(4)S	このコマンドが導入されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 destination-guard policy コマンドを使用して IPv6 宛先ガードを設定した場合、その後 IPv6 第 1 ホップ セキュリティ バインディング テーブルのリカバリを設定できます。

ipv6 snooping policy コマンドによりスヌーピング ポリシーを設定できます。 このポリシーの一部として第 1 ホップ セキュリティ バインディング テーブルのリカバリを設定できます。 スヌーピング ポリシーは **ipv6 snooping attach-policy** コマンドを使用して、ポートまたは VLAN に適用する必要があります。

destination-glean コマンドと **log-only** キーワードを使用した場合、syslog メッセージだけが生成され、リカバリは試行されません。

例

次の例では、宛先アドレスを DHCP からリカバリする必要があることを示します。

```
Device(config-ipv6-snooping)# destination-glean recovery dhcp
```

次の例では、バインディング テーブルのリカバリ後に欠落したすべての宛先アドレスについて syslog メッセージが生成されます。

```
Device(config-ipv6-snooping)# destination-glean log-only
```

関連コマンド

コマンド	説明
ipv6 destination-guard policy	IPv6 宛先ガード ポリシーを設定します。
ipv6 snooping policy	IPv6 スヌーピング コンフィギュレーション モードを開始します。

device-role

ポートに接続されているデバイスのロールを指定するには、ネイバー探索（ND）インスペクション ポリシー コンフィギュレーション モードまたはルータ アドバタイズメント（RA）ガード ポリシー コンフィギュレーション モードで **device-role** コマンドを使用します。

device-role {**host**| **monitor**| **router**}

構文の説明

host	デバイスのロールをホストに設定します。
monitor	デバイスのロールをモニタに設定します。
router	デバイスのロールをルータに設定します。

コマンド デフォルト

デバイスのロールはホストです。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション（config-nd-inspection）

RA ガード ポリシー コンフィギュレーション（config-ra-guard）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.2(4)S	このコマンドが Cisco IOS Release 15.2(4)S に統合されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

device-role コマンドは、ポートに接続されたデバイスのロールを指定します。 デフォルトでは、デバイスのロールはホストであるため、すべてのインバウンドルータ アドバタイズメントとリダイレクト メッセージはブロックされます。 **router** キーワードを使用してデバイス ロールをイネーブルにすると、このポートで、すべてのメッセージ（ルータ送信要求（RS）、ルータ アドバタイズメント（RA）、またはリダイレクト）が許可されます。

router または **monitor** キーワードが使用されている場合、制限付きブロードキャストがイネーブルかどうかに関係なく、マルチキャスト RS メッセージがポートでブリッジングされます。 ただし、**monitor** キーワードはインバウンド RA またはリダイレクト メッセージを許可しません。 **monitor** キーワードを使用すると、必要とするデバイスがこれらのメッセージを受け取ります。

（注） Cisco IOS Release 15.2(4) S1 から、信頼できるポートがデバイス ロールよりも優先して、ポート上でルータへの RA を受信します。 このリリース以前は、デバイス ロールのルータが信頼できるポートよりも優先されていました。デバイス ロールのルータは、RS をポートに送信できるようにするために、現在も設定する必要があります。

例

次に、ネイバー探索プロトコル（NDP）ポリシー名を policy1 として定義し、デバイスを ND インスペクション ポリシー コンフィギュレーション モードにして、ホストとしてデバイスを設定する例を示します。

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# device-role host
```

次に、RA ガード ポリシー名を raguard1 として定義し、デバイスを RA ガード ポリシー コンフィギュレーション モードにして、ホストとしてデバイスを設定する例を示します。

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# device-role host
```

関連コマンド

コマンド	説明
ipv6 nd inspection policy	ND インスペクション ポリシー名を定義して、ND インスペクション ポリシー コンフィギュレーション モードを開始します。
ipv6 nd raguard policy	RA ガード ポリシー名を定義し、RA ガード ポリシー コンフィギュレーション モードを開始します。

drop-unsecure

オプションがないか、無効なオプションまたは無効なシグニチャが含まれるメッセージをドロップするには、ネイバー探索（ND）インスペクション ポリシー コンフィギュレーション モードまたはルータ アドバタイズメント（RA）ガード ポリシー コンフィギュレーション モードで **drop-unsecure** コマンドを使用します。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

drop-unsecure

no drop-unsecure

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ND インスペクション ポリシーは設定されていません。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション（config-nd-inspection）

RA ガード ポリシー コンフィギュレーション（config-ra-guard）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

drop-unsecure コマンドは、RFC 3971『*Secure Discovery (SeND)*』に従い、暗号化生成アドレス（CGA）オプションまたは Rivest, Shamir, and Adleman（RSA）シグニチャがない、または無効であるメッセージをドロップします。 ただし、RFC 3972『*Cryptographically Generated Addresses (CGA)*』に準拠していない、または同RFCに従って検証されていないRSAシグニチャまたはCGAオプションが含まれているメッセージがドロップされることに注意してください。

drop-unsecure コマンドは、**ipv6 nd inspection policy** コマンドを使用して ND インスペクション ポリシー コンフィギュレーション モードをイネーブルにした後で使用します。

例

次に、NDポリシー名をpolicy1として定義し、ルータをNDインスペクション ポリシー コンフィギュレーション モードにして、無効なCGAオプションまたは無効なRSAシグニチャを含むメッセージをドロップするようルータをイネーブルにする例を示します。

```
Router(config)# ipv6 nd-inspection policy policy1
Router(config-nd-inspection)# drop-unsecure
```

関連コマンド

コマンド	説明
ipv6 nd inspection policy	NDインスペクション ポリシー名を定義して、NDインスペクション ポリシー コンフィギュレーション モードを開始します。
ipv6 nd raguard policy	RAガード ポリシー名を定義し、RAガード ポリシー コンフィギュレーション モードを開始します。

enforcement

宛先ガード ポリシーの適用レベルを設定するには、宛先ガード コンフィギュレーション モードで **enforcement** コマンドを使用します。

enforcement {**always**| **stressed**}

構文の説明

always	適用レベルを常時に設定します。
stressed	適用レベルをシステムにストレスがある場合にだけ適用するように設定します。

コマンド デフォルト

宛先ガード ポリシーの適用レベルは常時に設定されます。

コマンド モード

宛先ガード コンフィギュレーション（config-destguard）

コマンド履歴

リリース	変更内容
15.2(4)S	このコマンドが導入されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ネットワーク アーキテクチャ、バインディング テーブル情報のソース、およびシステムの変更の程度によっては、バインディング テーブルに VLAN のノード メンバーシップに関する詳細な情報が常にあるわけではない可能性があります。 適用レベル ポリシー要素は、VLAN メンバーシップに関して信頼される情報を持つシステムでは、適用レベルを always に設定する必要があることを意味します。 信頼性の低くてもよいシステム、または不用意なパケット損失を強く回避したいシステムでは、適用レベルを stressed に設定します

例

次に、適用レベルを常時に設定する例を示します。

```
Device(config)# ipv6 destination-guard policy destination
Device(config-destguard)# enforcement always
```

関連コマンド

コマンド	説明
ipv6 destination-guard policy	宛先ガード ポリシーを定義します。

graceful-restart

グレースフル リスタート対応ルータで Open Shortest Path First バージョン 3（OSPFv3）のグレースフル リスタート機能をイネーブルにするには、OSPF ルータ コンフィギュレーション モードで **graceful-restart** コマンドを使用します。 グレースフル リスタートをディセーブルにするには、このコマンドの **no** 形式を使用します。

graceful-restart [**restart-interval** *interval*]

no graceful-restart

構文の説明

restart-interval *interval*	（任意）秒単位の、グレースフル リスタートの間隔。 指定できる範囲は 1 ～ 1800 で、デフォルトは 120 です。

コマンド デフォルト

GR 対応ルータで GR 機能はイネーブルになっていません。

コマンド モード

OSPFv3 ルータ コンフィギュレーション モード（config-router）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが導入されました。
15.0(1)M	このコマンドが、Cisco IOS Release 12.5(1)M に統合されました。
12.2(33)SRE	このコマンドが変更されました。 Cisco IOS Release 12.2(33)SRE に統合されました。
12.2(33)XNE	このコマンドが変更されました。 Cisco IOS Release 12.2(33)XNE に統合されました。
15.1(3)S	このコマンドが変更されました。 機能は、IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
Cisco IOS XE Release 3.4S	このコマンドが変更されました。 機能は、IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
15.2(1)T	このコマンドが変更されました。 機能は、IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。

リリース	変更内容
15.1(1)SY	このコマンドが変更されました。 機能は、IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

graceful-restart コマンドは GR 対応ルータでだけイネーブルにできます。

例

次に、IPv6 および IPv4 で、GR 対応ルータでグレースフル リスタート モードをイネーブルにする例を示します。

```
Router(config)# ospfv3 router 1
Router(config-router)# graceful-restar
```

次に、IPv6 でのみ、GR 対応ルータでグレースフル リスタート モードをイネーブルにする例を示します。

```
Router(config)# ipv6 router ospf 1234
Router(config-router)# graceful-restart
```

関連コマンド

コマンド	説明
graceful-restart helper	GR 対応ルータで OSPFv3 グレースフル リスタート機能をイネーブルにします。
router ospfv3	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。

hop-limit

アドバタイズされたホップ カウント制限を確認するには、RA ガード ポリシー コンフィギュレーション モードで **hop-limit** コマンドを使用します。

hop-limit {**maximum**| **minimum** } *limit*

構文の説明

maximum *limit*	ホップ カウント制限が *limit* 引数によって設定された値よりも低いことを確認します。
minimum *limit*	ホップ カウント制限が *limit* 引数によって設定された値よりも大きいことを確認します。

コマンド デフォルト

ホップ カウント制限は指定されていません。

コマンド モード

RA ガード ポリシー コンフィギュレーション（config-ra-guard）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.2(4)S	このコマンドが Cisco IOS Release 15.2(4)S に統合されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

hop-limit コマンドによって、アドバタイズされたホップ カウント制限が *limit* 引数によって設定された値より大きいまたは小さいことを確認できます。 **minimum** キーワードと *limit* 引数を設定すると、攻撃者がホストに低いホップ カウント制限値を設定して、リモート接続先（デフォルト ルータの先）にトラフィックを生成できないようにすることを防止できます。 アドバタイズされたホップ カウント制限値が指定されていない場合（値 0 を設定した場合と同じ）、パケットはドロップされます。

maximum キーワードと *limit* 引数を設定すると、アドバタイズされたホップ カウント制限が *limit* 引数で設定した値未満であることを確認できます。アドバタイズされたホップカウント制限値が指定されていない場合（値 0 を設定した場合と同じ）、パケットはドロップされます。

例

次に、ルータ アドバタイズメント（RA）ガード ポリシー名を raguard1 として定義し、ルータを RA ガード ポリシー コンフィギュレーション モードにして、最小ホップ カウント制限を 3 に設定する例を示します。

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# hop-limit minimum 3
```

関連コマンド

コマンド	説明
ipv6 nd raguard policy	RA ガード ポリシー名を定義し、RA ガード ポリシー コンフィギュレーション モードを開始します。

interval-option

RA スロットル ポリシーの IPv6 ルータ アドバタイズメント（RA）間隔を調整するには、IPv6 RA スロットル ポリシー コンフィギュレーション モードで **interval-option** を使用します。 コマンドをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

interval-option {**ignore**| **inherit**| **pass-through**| **throttle**}

構文の説明

ignore	間隔オプションはスロットリングに影響しません。
inherit	ターゲット ポリシー間の設定をマージします。
pass-through	間隔オプションを持つすべての RA が転送されます。
throttle	間隔オプションを持つすべての RA がスロットリングされます。

コマンド デフォルト

Pass-through

コマンド モード

IPv6 RA スロットル ポリシー コンフィギュレーション モード（config-nd-ra-throttle）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

interval-option コマンドは、RA スロットル ポリシーの間隔オプションを設定します。 RFC 6275 で定義されているように、間隔オプションは、送信側デバイスが非送信請求マルチキャスト RA を送信する間隔をアドバタイズするために RA メッセージで使用されます。

例

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# interval-option inherit
```

ipv6 access-list

IPv6 アクセス リストを定義してデバイスを IPv6 アクセス リスト コンフィギュレーション モードに設定するには、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用します。 アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

ipv6 access-list *access-list-name*

no ipv6 access-list *access-list-name*

構文の説明

access-list-name	IPv6 アクセス リスト名。 名前は、スペース、疑問符を含むことができず、また、数字で始めることはできません。

コマンド デフォルト

IPv6 アクセス リストは定義されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.0(23)S	IPv6 アドレス コンフィギュレーション モードおよび拡張アクセス リスト機能（IPv6 オプション ヘッダー、およびオプションで上位層プロトコル タイプ情報に基づくトラフィック フィルタリング）のサポートが追加されました。 さらに、次のキーワードと引数がグローバル コンフィギュレーション モードから IPv6 アクセス リスト コンフィギュレーション モードに移動されました。**permit**、**deny**、*source-ipv6-prefix* / *prefix-length*、**any**、*destination-ipv6-prefix* / *prefix-length*、**priority**。 詳細については、「使用上のガイドライン」の項を参照してください。

リリース	変更内容
12.2(13)T	IPv6アドレス コンフィギュレーション モードおよび拡張アクセス リスト機能（IPv6 オプション ヘッダー、およびオプションで上位層プロトコル タイプ情報に基づくトラフィック フィルタリング）のサポートが追加されました。 さらに、次のキーワードと引数がグローバル コンフィギュレーション モードから IPv6 アクセス リスト コンフィギュレーション モードに移動されました。**permit**、**deny**、*source-ipv6-prefix* / *prefix-length*、**any**、*destination-ipv6-prefix* / *prefix-length*、**priority**。 詳細については、「使用上のガイドライン」の項を参照してください。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	重複する remark ステートメントは、IPv6 アクセス コントロール リストでは設定できません。
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ デバイスで追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

IPv6 固有である点を除くと、**ipv6 access-list** コマンドは **ip access-list** コマンドと類似しています。

Cisco IOS Release 12.2(2)T 以降のリリース、12.0(21)ST、および 12.0(22)S では、標準の IPv6 アクセス コントロール リスト（ACL）機能が基本的なトラフィック フィルタリング機能に使用されます。トラフィック フィルタリングは、送信元アドレスと宛先アドレス、特定のインターフェイスへのインバウンドおよびアウトバウンド、各アクセス リストの末尾にある暗黙的な deny ステートメントに基づきます（IPv4 の標準の ACL に似た機能）。 IPv6 ACL を定義し、拒否条件と許可条件を設定するには、グローバル コンフィギュレーション モードで **deny** キーワードと **permit** キーワードを指定して **ipv6 access-list** コマンドを使用します。

Cisco IOS Release 12.0(23)S 以降のリリースでは、標準の IPv6 ACL 機能が拡張されています。送信元および宛先アドレスに基づくトラフィック フィルタリングに加えて、IPv6オプションヘッダー、およびオプションでより細かい制御を行うための上位層プロトコルタイプ情報に基づくトラフィック フィルタリングがサポートされています（IPv4 の拡張 ACL に似た機能）。 IPv6 ACL は **ipv6 access-list** コマンドをグローバル コンフィギュレーション モードで使用することにより定義され、その許可と拒否の条件は **deny** および **permit** コマンドを IPv6 アクセス リスト コンフィギュレーション モードで使用することにより設定されます。 **ipv6 access-list** コマンドを設定すると、デバイスが IPv6 アクセス リスト コンフィギュレーション モードに設定され、プロンプト device は

Device(config-ipv6-acl)# に変わります。 IPv6 アクセス リスト コンフィギュレーション モードから、定義済みの IPv6 ACL に許可および拒否の条件を設定できます。

（注） IPv6 ACL は一意な名前によって定義されます（IPv6 は番号付けされた ACL をサポートしません）。 IPv4 ACL と IPv6 ACL は同じ名前を共有できません。

Cisco IOS Release 12.0(23)S 以降のリリースおよび 12.2(11)S 以降のリリースでは、下位互換性のために、グローバル コンフィギュレーション モードでの **deny** キーワードと **permit** キーワードを指定した **ipv6 access-list** コマンドが引き続きサポートされています。ただし、グローバル コンフィギュレーション モードで拒否条件と許可条件を使用して定義された IPv6 ACL は、IPv6 アクセス リスト コンフィギュレーション モードに変換されます。

IPv6 オプション ヘッダーおよび任意の上位層プロトコル タイプ情報に基づいて IPv6 トラフィックをフィルタリングする方法の詳細については、deny（IPv6）コマンドおよびpermit（IPv6）コマンドを参照してください。 変換された IPv6 ACL の設定例については、「例」の項を参照してください。

（注） Cisco IOS Release 12.0(23)S 以降のリリースでは、IPv6 ACL に最後の一致条件として暗黙の **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および**deny ipv6 any any** ステートメントがあります。（前の 2 つの一致条件により ICMPv6 ネイバー探索が可能になります）。IPv6 ACL には、暗黙の **deny ipv6 any any** ステートメントを有効にするために少なくとも 1 つのエントリが含まれる必要があります。 IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを利用するため、デフォルトで、インターフェイス上での IPv6 ネイバー探索パケットの送受信が IPv6 ACL によって暗黙的に許可されます。 IPv4 の場合、IPv6 ネイバー探索プロセスに相当するアドレス解決プロトコル（ARP）では、個別のデータ リンク層プロトコルを利用するため、デフォルトで、インターフェイス上での ARP パケットの送受信が IPv4 ACL によって暗黙的に許可されます。

（注） アクセス リストでなく、IPv6 プレフィックス リストは、ルーティング プロトコル プレフィックスのフィルタリングに使用する必要があります。

IPv6 ACL を IPv6 インターフェイスに適用するには、*access-list-name* 引数を指定して **ipv6 traffic-filter** インターフェイス コンフィギュレーション コマンドを使用します。 デバイスとの間で入力および出力 IPv6 仮想端末接続に IPv6 ACL を適用するには、*access-list-name* 引数を指定して **ipv6 access-class** ライン コンフィギュレーション コマンドを使用します。

（注） **ipv6 traffic-filter** コマンドでインターフェイスに適用された IPv6 ACL は、デバイスから発信されるトラフィックではなく、転送されるトラフィックをフィルタリングします。

（注） このコマンドを使用してブートストラップ ルータ（BSR）候補ランデブー ポイント（RP）（**ipv6 pim bsr candidate rp** コマンドを参照）、またはスタティック RP（**ipv6 pim rp-address** コマンドを参照）にすでに関連付けられている ACL を変更する場合、PIM SSM グループ アドレス範囲（FF3x::/96）に重複する追加されたアドレス範囲は無視されます。警告メッセージが生成され、重複するアドレス範囲は ACL に追加されますが、設定された BSR 候補 RP またはスタティック RP コマンドの動作には影響を与えません。

Cisco IOS Release 12.2(33)SXH およびそれに続く Cisco IOS SX リリースでは、重複した remark ステートメントは、IPv6 アクセス コントロール リストでは設定できません。 各 remark ステートメントは別のエンティティであるため、それぞれが一意である必要があります。

例

次に、Cisco IOS Release 12.0(23)S 以降のリリースを実行するデバイスからの例を示します。 この例では、list1 という IPv6 ACL リストを設定し、デバイスを IPv6 アクセス リスト コンフィギュレーション モードにします。

```
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)#
```

次に、Cisco IOS Release 12.2(2)T 以降のリリース、12.0(21)ST、または 12.0(22)S を実行するデバイスからの例を示します。 この例では、list2 という名前の IPv6 ACL を設定し、その ACL をイーサネット インターフェイス 0 上の発信トラフィックに適用します。 特に、最初の ACL エントリは、ネットワーク FEC0:0:0:2::/64（送信元 IPv6 アドレスの最初の 64 ビットとしてサイトローカル プレフィックス FEC0:0:0:2 を持つパケット）がイーサネット インターフェイス 0 から出て行くことを拒否します。 2 番めの ACL エントリは、その他のすべてのトラフィックがイーサネット インターフェイス 0 から出て行くことを許可します。 2 番めのエントリは、各 IPv6 ACL の末尾に暗黙的な deny all 条件があるため、必要となります。

```
Device(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Device(config)# ipv6 access-list list2 permit any any
Device(config)# interface ethernet 0
Device(config-if)# ipv6 traffic-filter list2 out
```

同じ設定が Cisco IOS Release 12.0(23)S 以降のリリースを実行しているデバイスで入力された場合、設定は、IPv6 アクセス リスト コンフィギュレーション モードに、次のように変換されます。

```
ipv6 access-list list2
  deny FEC0:0:0:2::/64 any
  permit ipv6 any any
interface ethernet 0
 ipv6 traffic-filter list2 out
```

（注） IPv6 は、グローバル コンフィギュレーション モードから IPv6 アクセス リスト コンフィギュレーション モードに変換される **permit any any** 文および **deny any any** 文でプロトコル タイプとして自動的に設定されます。

（注） Cisco IOS Release 12.2(2)T 以降のリリース、12.0(21)ST または 12.0(22)S を実行するデバイスで定義され、暗黙の拒否条件に依存するか、トラフィックをフィルタリングする **deny any any** ステートメントを指定する IPv6 ACL には、プロトコル パケット（ネイバー探索プロトコルに関連付けられたパケットなど）のフィルタリングを避けるため、リンクローカル アドレスおよびマルチキャスト アドレスに対する **permit** ステートメントを含める必要があります。 また、**deny** ステートメントを使用してトラフィックをフィルタリングする IPv6 ACL では、**permit any any** ステートメントをリストの最後のステートメントとして使用する必要があります。

（注） IPv6 デバイスは、送信元または宛先アドレスのいずれかとしてリンクローカル アドレスを持つIPv6パケットを別のネットワークに転送しません（パケットの送信元インターフェイスは、パケットの宛先インターフェイスとは異なります）。

関連コマンド

コマンド	説明
deny（IPv6）	IPv6アクセス リストに拒否条件を設定します。
ipv6 access-class	IPv6 アクセス リストに基づいて、デバイスとの間で着信接続および発信接続をフィルタリングします。
ipv6 pim bsr candidate rp	BSR に PIM RP アドバタイズメントを送信するように候補 RP を設定します。
ipv6 pim rp-address	特定のグループ範囲の PIM RP のアドレスを設定します。
ipv6 traffic-filter	インターフェイス上の着信または発信 IPv6 トラフィックをフィルタリングします。
permit（IPv6）	IPv6アクセス リストに許可条件を設定します。
show ipv6 access-list	現在のすべての IPv6 アクセス リストの内容を表示します。

ipv6 address

IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 address** コマンドを使用します。 インターフェイスからアドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address {*ipv6-prefix/prefix-length*| *prefix-name sub-bits/prefix-length*}

no ipv6 address {*ipv6-address/prefix-length*| *prefix-name sub-bits/prefix-length*}

構文の説明

ipv6-address	使用する IPv6 アドレス。
/ *prefix-length*	IPv6 プレフィックスの長さ。 プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す10進値です。10 進数値の前にスラッシュ記号が必要です。
prefix-name	インターフェイスに設定するネットワークの上位ビットを指定する一般的なプレフィックス。
sub-bits	*prefix-name* 引数で指定された一般的なプレフィックスによって提供されるプレフィックスと連結されるアドレスのサブプレフィックス ビットおよびホスト ビット。 *sub-bits* 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。

コマンド デフォルト

IPv6 アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。

リリース	変更内容
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズ デバイスに統合されました。
15.2(4)S	このコマンドが Cisco IOS Release 15.2(4)S に統合されました。
15.2(2)SNG	このコマンドが、Cisco ASR 901 シリーズのアグリゲーション サービス デバイスに実装されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 address コマンドは、さまざまなオプションを使用し、さまざまな方法で、複数の IPv6 アドレスをインターフェイスで設定できます。 最も一般的な方法は、IPv6 アドレスとプレフィックスの長さを指定する方法です。

アドレスは、サブプレフィックスおよびホスト ビットから集約された IPv6 プレフィックス ビットを区切る一般的なプレフィックスのメカニズムを使用して定義することもできます。 この場合、アドレスの上位ビットは、グローバルに設定または学習される一般的なプレフィックスで定義されます（Dynamic Host Configuration Protocol プレフィックス委任（DHCP-PD）を使用し、*prefix-name* 引数を使用して適用するなど）。 サブプレフィックス ビットおよびホスト ビットは *sub-bits* 引数を使用して定義されます。

引数を指定せずに **no ipv6 address autoconfig** コマンドを使用すると、インターフェイスからすべての IPv6 アドレスが削除されます。

インターフェイスで **ipv6 address link-local** コマンドを使用して、IPv6 リンクローカル アドレスを設定し、IPv6 処理をイネーブルにする必要があります。

例

次に、インターフェイスで IPv6 処理をイネーブルにし、一般的なプレフィックス my-prefix と直接指定したビットに基づいてアドレスを設定する例を示します。

```
Device(config-if) ipv6 address my-prefix 0:0:0:7272::72/64
```

my-prefix という名前の一般的なプレフィックスの値が 2001:DB8:2222::/48 であるとすると、グローバル アドレス 2001:DB8:2222:7272::72/64 でインターフェイスを設定する必要があります。

関連コマンド

コマンド	説明
ipv6 address anycast	IPv6 エニーキャスト アドレスを設定し、インターフェイスで IPv6 処理をイネーブルにします。
ipv6 address eui-64	IPv6アドレスを設定して、そのアドレスの下位64 ビットの EUI-64 インターフェイス ID を使用して、インターフェイスでの IPv6 処理をイネーブルにします。
ipv6 address link-local	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ipv6 unnumbered	インターフェイスに明示的な IPv6 アドレスを割り当てなくても、インターフェイスで IPv6 処理をイネーブルにします。
no ipv6 address autoconfig	インターフェイスからすべての IPv6 アドレスを削除します。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 address anycast

IPv6エニーキャストアドレスを設定し、インターフェイスでIPv6処理をイネーブルにするには、インターフェイス コンフィギュレーション モードで**ipv6 address anycast**コマンドを使用します。インターフェイスからアドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address *ipv6-prefix/prefix-length* **anycast**

no ipv6 address [*ip6-prefix/prefix-length* **anycast**]

構文の説明

ipv6-prefix	インターフェイスに割り当てられた IPv6 ネットワーク。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの16ビット値を使用して、アドレスを 16 進数で指定します。
/ prefix-length	IPv6 プレフィックスの長さ。 プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す10進値です。10 進数値の前にスラッシュ記号が必要です。

コマンド デフォルト

IPv6 アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.3(4)T	このコマンドが導入されました。
12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。

リリース	変更内容
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

引数を指定せずに **no ipv6 address** コマンドを使用すると、手動で設定したすべての IPv6 アドレスがインターフェイスから削除されます。

例

次に、インターフェイスで IPv6 処理をイネーブルにし、プレフィックス 2001:0DB8:1:1::/64 をインターフェイスに割り当て、IPv6 エニーキャスト アドレス 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE を設定する例を示します。

```
ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast
```

関連コマンド

コマンド	説明
ipv6 address eui-64	IPv6アドレスを設定して、そのアドレスの下位64 ビットの EUI-64 インターフェイス ID を使用して、インターフェイスでの IPv6 処理をイネーブルにします。
ipv6 address link-local	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ipv6 unnumbered	インターフェイスに明示的な IPv6 アドレスを割り当てなくても、インターフェイスで IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 address autoconfig

インターフェイスでステートレス自動設定を使用する IPv6 アドレスの自動設定をイネーブルにし、インターフェイスでIPv6処理をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 address autoconfig** コマンドを使用します。 インターフェイスからアドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address autoconfig [default]

no ipv6 address autoconfig

構文の説明

default	（任意）デフォルトのデバイスがこのインターフェイスで選択されている場合、**default** キーワードによって、デフォルト ルートがそのデフォルトデバイスを使用してインストールされます。 **default** キーワードは、1 個のインターフェイスでのみ指定できます。

コマンド デフォルト

IPv6 アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(13)T	このコマンドが導入されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
Cisco IOS XE Release 2.5	このコマンドが、Cisco IOS XE Release 2.5 に統合されました。
12.2(33)XNE	このコマンドが、Cisco IOS Release 12.2(33)XNE に統合されました。
15.1(2)SNG	このコマンドが、Cisco ASR 901 シリーズのアグリゲーション サービス デバイスに実装されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 address autoconfig コマンドによって、デバイスは IPv6 ステートレス アドレス自動設定を実行し、リンクのプレフィックスを検出してインターフェイス EUI-64 ベースのアドレスを追加します。アドレスは、ルータ アドバタイズメント（RA）メッセージで受信したプレフィックスによって設定されます。

引数を指定せずに **no ipv6 address autoconfig** コマンドを使用すると、インターフェイスからすべての IPv6 アドレスが削除されます。

例

次に、IPv6 アドレスを自動的に割り当てる例を示します。

```
Device(config)# interface ethernet 0
Device(config-if)# ipv6 address autoconfig
```

関連コマンド

コマンド	説明
ipv6 address eui-64	IPv6アドレスを設定して、そのアドレスの下位64 ビットの EUI-64 インターフェイス ID を使用して、インターフェイスでの IPv6 処理をイネーブルにします。
ipv6 address link-local	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ipv6 unnumbered	インターフェイスに明示的な IPv6 アドレスを割り当てなくても、インターフェイスで IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 address dhcp

Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバからインターフェイスの IPv6 アドレスを取得するには、インターフェイス コンフィギュレーション モードで **ipv6 address dhcp** コマンドを使用します。 インターフェイスからアドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address dhcp [rapid-commit]

no ipv6 address dhcp

構文の説明

rapid-commit	（任意）アドレス割り当て用に 2 メッセージ交換方式を許可します。

コマンド デフォルト

IPv6 アドレスは、DHCPv6 サーバから取得されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.4(24)T	このコマンドが導入されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 address dhcp インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイスは DHCP を使用して IPv6 アドレスを動的に学習できます。

rapid-commit キーワードは、アドレス割り当ておよびその他の設定について、2 つのメッセージ交換を使用できるようにします。 これをイネーブルにすると、クライアントは送信請求メッセージに rapid-commit オプションを含めます。

例

次に、IPv6 アドレスを取得して、rapid-commit オプションをイネーブルにする例を示します。

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ipv6 address dhcp
rapid-commit
```

特権 EXEC モードで **show ipv6 dhcp interface** コマンドを使用すると、設定を確認できます。

関連コマンド

コマンド	説明
show ipv6 dhcp interface	DHCPv6 インターフェイスの情報を表示します。

ipv6 address eui-64

インターフェイスに IPv6 アドレスを設定し、アドレスの下位 64 ビットで EUI-64 インターフェイス ID を使用してインターフェイスでの IPv6 処理をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 address eui-64** コマンドを使用します。 インターフェイスからアドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address *ipv6-prefix/prefix-length* **eui-64**

no ipv6 address [*ip v6-prefix/prefix-length* **eui-64**]

構文の説明

ipv6-prefix	インターフェイスに割り当てられた IPv6 ネットワーク。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
/ prefix-length	IPv6 プレフィックスの長さ。 プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す10進値です。10 進数値の前にスラッシュ記号が必要です。

コマンド デフォルト

IPv6 アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。

リリース	変更内容
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ ルータで追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

/ *prefix-length* 引数に指定される値が、64 ビットを超える場合、プレフィックス ビットは、インターフェイス ID より優先されます。

引数を指定せずに no ipv6 address コマンドを使用すると、手動で設定したすべての IPv6 アドレスがインターフェイスから削除されます。

Cisco IOS ソフトウェアが、その IPv6 アドレスのいずれかを使用する別のホストを検出すると、コンソールにエラー メッセージを表示します。

例

次に、IPv6 アドレス 2001:0DB8:0:1::/64 をイーサネット インターフェイス 0 に割り当て、アドレスの下位 64 ビットの EUI-64 インターフェイス ID を指定する例を示します。

```
Router(config)# interface ethernet 0
Router(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
```

関連コマンド

コマンド	説明
ipv6 address link-local	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ipv6 unnumbered	インターフェイスに明示的な IPv6 アドレスを割り当てなくても、インターフェイスで IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 address link-local

インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 address link-local** コマンドを使用します。インターフェイスからアドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address *ipv6-address/prefix-length* **link-local [cga]**

no ipv6 address [*ipv6-address/prefix-length* **link-local**]

構文の説明

ipv6-address	インターフェイスに割り当てられた IPv6 アドレス。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
/ *prefix-length*	IPv6 プレフィックスの長さ。 プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
link-local	リンクローカル アドレスを指定します。 このコマンドに指定された *ipv6-address* は、インターフェイス用に自動的に生成されるリンクローカル アドレスを上書きします。
cga	（任意）CGA インターフェイス ID を指定します。

コマンド デフォルト

IPv6 アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。

リリース	変更内容
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ ルータで追加されました。
12.4(24)T	**cga** キーワードが追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

引数を指定せずに **no ipv6 address** コマンドを使用すると、手動で設定したすべての IPv6 アドレスがインターフェイスから削除されます。

Cisco ソフトウェアが、その IPv6 アドレスのいずれかを使用する別のホストを検出すると、コンソールにエラー メッセージを表示します。

IPv6 処理がインターフェイスでイネーブルにされていて、通常、IPv6 アドレスがインターフェイスで設定されている場合、インターフェイスのリンクローカル アドレスが自動的に生成されます。インターフェイスで使用されるリンクローカルアドレスを手動で指定するには、ipv6 address link-local コマンドを使用します。

連続する 16 ビット値がゼロとして指定されている場合は、2 つのコロンを *ipv6-address* 引数の一部として使用できます。インターフェイスごとに複数のIPv6アドレスを設定できますが、設定できるリンクローカル アドレスは 1 つだけです。

例

次に、イーサネットインターフェイス0のリンクローカルアドレスとしてFE80::260:3EFF:FE11:6770を割り当てる例を示します。

```
interface ethernet 0
 ipv6 address FE80::260:3EFF:FE11:6770 link-local
```

関連コマンド

コマンド	説明
ipv6 address eui-64	IPv6アドレスを設定して、そのアドレスの下位64ビットのEUI-64インターフェイスIDを使用して、インターフェイスでのIPv6処理をイネーブルにします。
ipv6 unnumbered	インターフェイスに明示的なIPv6アドレスを割り当てなくても、インターフェイスでIPv6処理をイネーブルにします。
show ipv6 interface	IPv6向けに設定されたインターフェイスの使用状況を表示します。

ipv6 cef

Cisco Express Forwarding for IPv6 をイネーブルにするには、グローバル コンフィギュレーション モードで **ipv6 cef** コマンドを使用します。 Cisco Express Forwarding for IPv6 をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 cef

no ipv6 cef

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

Cisco Express Forwarding for IPv6 はデフォルトでディセーブルです。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.0(22)S	このコマンドが導入されました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータに実装されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 cef コマンドは **ip cef** コマンドと類似していますが、これは IPv6 専用です。

ipv6 cef コマンドは、Cisco 12000 シリーズ インターネット ルータでは使用できません。この分散プラットフォームは、分散型 Cisco Express Forwarding for IPv6 モードでだけ動作するためです。

（注） **ipv6 cef** コマンドはインターフェイス コンフィギュレーション モードでサポートされません。

（注） Cisco 7500 シリーズ ルータなど一部の分散型アーキテクチャ プラットフォームは、Cisco Express Forwarding for IPv6 と分散型 Cisco Express Forwarding for IPv6 の両方をサポートします。 Cisco Express Forwarding for IPv6 が分散プラットフォームで設定されている場合、シスコ エクスプレス フォワーディング スイッチングはルート プロセッサ（RP）によって実行されます。

（注） **ipv6 cef** グローバル コンフィギュレーション コマンドを使用して Cisco Express Forwarding for IPv6 をイネーブルにする前に、**ip cef** グローバル コンフィギュレーション コマンドを使用して、Cisco Express Forwarding for IPv4 をイネーブルにする必要があります。

Cisco Express Forwarding for IPv6 は高度なレイヤ 3 IP スイッチング テクノロジーで、Cisco Express Forwarding for IPv4 と同じように機能し、同じ利点があります。 Cisco Express Forwarding for IPv6 は Web ベースのアプリケーションおよび対話型セッションに関連付けられているような、動的でトポロジ的に分散したトラフィック パターンを持つネットワークのパフォーマンスおよびスケーラビリティを最適化します。

例

次に、標準の Cisco Express Forwarding for IPv4 の動作と標準の Cisco Express Forwarding for IPv6 の動作をルータでグローバルにイネーブルにする例を示します。

```
ip cef
ipv6 cef
```

関連コマンド

コマンド	説明
ip route-cache	IP ルーティングの高速スイッチング キャッシュの使用を制御します。
ipv6 cef accounting	Cisco Express Forwarding for IPv6 および分散型 Cisco Express Forwarding for IPv6 のネットワーク アカウンティングをイネーブルにします。
ipv6 cef distributed	IPv6 での分散型シスコ エクスプレス フォワーディングをイネーブルにします。

コマンド	説明
show cef	ラインカードがドロップしたパケットまたは高速転送されなかったパケットを表示します。
show ipv6 cef	IPv6 FIB のエントリを表示します。

ipv6 cef accounting

ネットワーク アカウンティング用に Cisco Express Forwarding for IPv6 および分散型 Cisco Express Forwarding for IPv6 をイネーブルにするには、グローバル コンフィギュレーション モードまたはインターフェイス コンフィギュレーション モードで **ipv6 cef accounting** コマンドを使用します。Cisco Express Forwarding for IPv6 のネットワーク アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 cef accounting *accounting-types*

no ipv6 cef accounting *accounting-types*

Specific Cisco Express Forwarding Accounting Information Through Interface Configuration Mode

ipv6 cef accounting non-recursive {**external| internal**}

no ipv6 cef accounting non-recursive {**external| internal**}

構文の説明

accounting-types	*accounting-types* 引数は、次のキーワードのうち少なくとも 1 つで置き換える必要があります。任意で、他のキーワードの一部またはすべてをこのキーワードの後に入力できますが、各キーワードを使用できるのはそれぞれ一度だけです。 • **load-balance-hash**：ロード バランシング ハッシュ バケット カウンタをイネーブルにします。 • **non-recursive**：非再帰的プレフィックスによるアカウンティングをイネーブルにします。 • **per-prefix**：宛先（またはプレフィックス）へのパケット数とバイト数のコレクションの高速転送をイネーブルにします。 • **prefix-length**：プレフィックス長によるアカウンティングをイネーブルにします。
non-recursive	非再帰的プレフィックスによるアカウンティングをイネーブルにします。 このキーワードは、別のキーワードを入力した後、グローバル コンフィギュレーション モードで使用する場合、省略可能です。*accounting-types* 引数を参照してください。

external	非再帰的外部ビンの入力トラフィックをカウントします。
internal	非再帰的内部ビンの入力トラフィックをカウントします。

コマンド デフォルト

Cisco Express Forwarding for IPv6 のネットワーク アカウンティングは、デフォルトでディセーブルです。

コマンド モード

グローバル コンフィギュレーション（config）インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.0(22)S	このコマンドが導入されました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(25)S	**non-recursive** および **load-balance-hash** キーワードが追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ ルータで追加されました。
12.4(20)T	このコマンドが、Cisco IOS Release 12.4(20)T に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 cef accounting コマンドは、**ip cef accounting** コマンドに似ていますが、IPv6 固有です。

Cisco Express Forwarding for IPv6 のネットワーク アカウンティングを設定すると、ネットワークで Cisco Express Forwarding for IPv6 トラフィック パターンの統計情報を収集することができます。

グローバル コンフィギュレーション モードで **ipv6 cef accounting** コマンドを使用して、Cisco Express Forwarding for IPv6 のネットワーク アカウンティングをイネーブルにする場合、アカウンティング情報は、Cisco Express Forwarding for IPv6 モードがイネーブルの場合はルート プロセッサ（RP）で、分散型 Cisco Express Forwarding for IPv6 モードがイネーブルの場合はラインカードで収集されます。 **show ipv6 cef** EXEC コマンドを使用して、収集したアカウンティング情報を表示できます。

直接接続されるネクスト ホップのプレフィックスの場合、**non-recursive** キーワードを使用すると、プレフィックスを通じてパケットとバイトのコレクションを高速転送できます。 このキーワードは、**ipv6 cef accounting** コマンドの他のキーワードを入力した後にグローバル コンフィギュレーション モードで使用する場合、省略可能です。

インターフェイス コンフィギュレーション モードでは、このコマンドはグローバル コンフィギュレーション コマンドと組み合わせて使用する必要があります。 インターフェイス コンフィギュレーション コマンドでは、統計情報の蓄積に 2 つの異なるビン（内部または外部）を指定することができます。 内部ビンがデフォルトで使用されます。 統計情報は、**show ipv6 cef detail** コマンドを使用して表示します。

宛先単位のロードバランシングでは、使用可能なパスのセットが分配される一連の 16 のハッシュ バケットが使用されます。 パケットのプロパティで動作するハッシュ関数が、使用するパスを含むバケットを選ぶために適用されます。 送信元と宛先の IP アドレスは、宛先単位のロード バランシングでバケットの選択に使用されるプロパティです。ハッシュ バケット単位のカウンタをイネーブルにするには、**ipv6 cef accounting** コマンドで **load-balance-hash** キーワードを使用します。ハッシュ バケット単位のカウンタを表示するには、**show ipv6 cef** *prefix* **internal** コマンドを入力します。

例

次に、直接接続されたネクスト ホップを持つプレフィックスの Cisco Express Forwarding for IPv6 アカウンティング情報の収集をイネーブルにする例を示します。

```
Router(config)# ipv6 cef accounting non-recursive
```

関連コマンド

コマンド	説明
ip cef accounting	シスコ エクスプレス フォワーディングのネットワーク アカウンティングをイネーブルにします（IPv4）。
show cef	**シスコ エクスプレス フォワーディングにより転送**されるパケットの情報を表示します。
show ipv6 cef	IPv6 FIB のエントリを表示します。

ipv6 cef distributed

分散型 Cisco Express Forwarding for IPv6 をイネーブルにするには、グローバル コンフィギュレーション モードで **ipv6 cef distributed** コマンドを使用します。 Cisco Express Forwarding for IPv6 をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 cef distributed

no ipv6 cef distributed

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

分散型 Cisco Express Forwarding for IPv6 は、Cisco 7500 シリーズ ルータではディセーブルで、Cisco 12000 シリーズ インターネット ルータではイネーブルです。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.0(22)S	このコマンドが導入されました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータに実装されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 cef distributed コマンドは、**ip cef distributed** コマンドに似ていますが、IPv6 固有です。

グローバル コンフィギュレーション モードで **ipv6 cef distributed** を使用することにより、ルータで分散型 Cisco Express Forwarding for IPv6 をグローバルにイネーブルにすると、ルート プロセッサ（RP）から分散型アーキテクチャ プラットフォームのラインカードに IPv6 パケットのシスコ エクスプレス フォワーディング処理が分配されます。

（注） **ipv6 cef distributed** コマンドは Cisco 12000 シリーズ インターネット ルータ上ではサポートされません。このプラットフォームでは、分散型 Cisco Express Forwarding for IPv6 がデフォルトでイネーブルにされているためです。

（注） ルータの分散型 Cisco Express Forwarding for IPv6 トラフィックを転送するには、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用してルータで IPv6 ユニキャスト データグラムの転送をグローバルに設定し、**ipv6 address** インターフェイス コンフィギュレーション コマンドでインターフェイスに IPv6 アドレスおよび IPv6 処理を設定します。

（注） **ipv6 cef distributed** グローバル コンフィギュレーション コマンドを使用して分散型 Cisco Express Forwarding for IPv6 をイネーブルにする前に、**ip cef distributed** グローバル コンフィギュレーション コマンドを使用して、分散型 Cisco Express Forwarding for IPv4 をイネーブルにする必要があります。

シスコ エクスプレス フォワーディングは、高度なレイヤ 3 IP スイッチング テクノロジーです。シスコ エクスプレス フォワーディングは Web ベースのアプリケーションおよび対話型セッションに関連付けられているような、動的でトポロジ的に分散したトラフィック パターンを持つネットワークのパフォーマンスおよびスケーラビリティを最適化します。

例

次に、分散型 Cisco Express Forwarding for IPv6 の操作をイネーブルにする例を示します。

```
ipv6 cef distributed
```

関連コマンド

コマンド	説明
ip route-cache	IP ルーティングの高速スイッチング キャッシュの使用を制御します。
show ipv6 cef	IPv6 FIB のエントリを表示します。

ipv6-i1

- ipv6 dhcp guard attach-policy, 65 ページ
- ipv6 dhcp guard policy, 67 ページ
- ipv6 dhcp ping packets, 69 ページ
- ipv6 dhcp server, 71 ページ
- ipv6 enable, 74 ページ
- ipv6 host, 76 ページ
- ipv6 icmp error-interval, 78 ページ
- ipv6 nd cache expire, 81 ページ
- ipv6 nd inspection, 83 ページ
- ipv6 nd inspection policy, 85 ページ
- ipv6 nd na glean, 87 ページ
- ipv6 nd nud retry, 88 ページ
- ipv6 nd ra-throttle attach-policy, 90 ページ
- ipv6 nd ra-throttle policy, 92 ページ
- ipv6 nd raguard attach-policy, 94 ページ
- ipv6 nd raguard policy, 96 ページ
- ipv6 nd router-preference, 98 ページ
- ipv6 nd suppress attach-policy, 100 ページ
- ipv6 nd suppress policy, 102 ページ
- ipv6 neighbor binding logging, 104 ページ
- ipv6 neighbor binding max-entries, 106 ページ
- ipv6 neighbor binding vlan, 108 ページ

- ipv6 neighbor tracking, 110 ページ
- ipv6 prefix-list, 112 ページ

ipv6 dhcp guard attach-policy

Dynamic Host Configuration Protocol for IPv6（DHCPv6）ガードポリシーを適用するには、インターフェイス コンフィギュレーション モードまたは VLAN コンフィギュレーション モードで **ipv6 dhcp guard attach-policy** コマンドを使用します。 DHCPv6 ガード ポリシーを適用解除するには、このコマンドの **no** 形式を使用します。

Syntax Available In Interface Configuration Mode

ipv6 dhcp guard [**attach-policy** [*policy-name*]] [**vlan** {**add**| **all**| **except**| **none**| **remove**} *vlan-id* [*... vlan-id*]]

no ipv6 dhcp guard [**attach-policy** [*policy-name*]] [**vlan** {**add**| **all**| **except**| **none**| **remove**} *vlan-id* [*... vlan-id*]]

Syntax Available In VLAN Configuration Mode

ipv6 dhcp guard attach-policy [*policy-name*]

no ipv6 dhcp guard attach-policy [*policy-name*]

構文の説明

policy-name	（任意）DHCPv6 ガード ポリシー名。
vlan	（任意）DHCPv6 ポリシーを VLAN に適用するように指定します。
add	（任意）指定した VLAN に DHCPv6 ガード ポリシーを適用します。
all	（任意）全 VLAN に DHCPv6 ガード ポリシーを適用します。
except	（任意）指定した VLAN を除くすべての VLAN に DHCPv6 ガード ポリシーを適用します。
none	（任意）指定した VLAN のいずれにも DHCPv6 ガード ポリシーを適用しません。
remove	（任意）指定した VLAN から DHCPv6 ガード ポリシーを削除します。
vlan-id	（任意）DHCP ガード ポリシーが適用される VLAN の ID。

コマンド デフォルト

DHCPv6 ガード ポリシーは適用されません。（config-if）

VLAN コンフィギュレーション（config-vlan）

コマンド履歴

リリース	変更内容
15.2(4)S	このコマンドが導入されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

このコマンドによって、インターフェイスまたは 1 つ以上の VLAN に DHCPv6 ポリシーを適用できます。 DHCPv6 ガード ポリシーは、不正な DHCP サーバおよび DHCP パケットをサーバからクライアントに転送するリレーエージェントからの応答およびアドバタイズメント メッセージをブロックするために使用できます。 クライアント メッセージまたはリレー エージェントによってクライアントからサーバに送信されたメッセージが妨げられることはありません。

例

次に、インターフェイスに DHCPv6 ガード ポリシーを適用する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 0/2/0
Router# switchport
Router(config-if)# ipv6 dhcp guard attach-policy pol1 vlan add 1
```

関連コマンド

コマンド	説明
ipv6 dhcp guard policy	DHCPv6 ガード ポリシー名を定義します。
show ipv6 dhcp guard policy	DHCPv6 ガード ポリシー情報を表示します。

ipv6 dhcp guard policy

Dynamic Host Configuration Protocol for IPv6（DHCPv6）ガードポリシー名を定義するには、グローバル コンフィギュレーション モードで **ipv6 dhcp guard policy** コマンドを使用します。 DHCPv6 ガード ポリシー名を削除するには、このコマンドの **no** 形式を使用します。

ipv6 dhcp guard policy [*policy-name*]

no ipv6 dhcp guard policy [*policy-name*]

構文の説明

policy-name	（任意）DHCPv6 ガード ポリシー名。

コマンド デフォルト

DHCPv6 ガード ポリシー名は定義されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
15.2(4)S	このコマンドが導入されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

このコマンドで、DHCPv6 ガード コンフィギュレーション モードを開始することができます。 DHCPv6 ガード ポリシーは、不正な DHCP サーバおよび DHCP パケットをサーバからクライアントに転送するリレーエージェントからの応答およびアドバタイズメント メッセージをブロックするために使用できます。 クライアント メッセージまたはリレー エージェントによってクライアントからサーバに送信されたメッセージが妨げられることはありません。

例

次に、DHCPv6 ガード ポリシー名を定義する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# ipv6 dhcp guard policy policy1
```

関連コマンド

コマンド	説明
show ipv6 dhcp guard policy	DHCPv6 ガード ポリシー情報を表示します。

ipv6 dhcp ping packets

Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバが ping 操作の一部としてプール アドレスに送信するパケットの数を指定するには、グローバル コンフィギュレーション モードで **ipv6 dhcp ping packets** コマンドを使用します。 サーバがプール アドレスに ping を送信しないようにするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp ping packets *number*

ipv6 dhcp ping packets

構文の説明

number	アドレスが要求元のクライアントに割り当てられる前に送信された ping パケット数。 有効値は 0 ～ 10 です。

コマンド デフォルト

アドレスが要求元クライアントに割り当てられる前に、ping パケットは送信されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.4(24)T	このコマンドが導入されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

DHCPv6 サーバは、要求元クライアントにアドレスを割り当てる前にプール アドレスに ping を送信します。 ping の応答がない場合、サーバはアドレスが使用されていない可能性が高いと想定し、アドレスを要求元クライアントに割り当てます。

number 引数を 0 に設定すると、DHCPv6 サーバの ping 操作がオフになります。

例

次の例では、DHCPv6 サーバで ping 試行を中止するまでに 4 回の ping を試行するように指定します。

```
Router(config)# ipv6 dhcp ping packets 4
```

関連コマンド

コマンド	説明
clear ipv6 dhcp conflict	DHCPv6 サーバデータベースからアドレス競合をクリアします。
show ipv6 dhcp conflict	DHCPv6 サーバによって検出された、またはクライアントから DECLINE メッセージにより報告されたアドレス競合を表示します。

ipv6 dhcp server

インターフェイスで IPv6 サービス用の Dynamic Host Configuration Protocol（DHCP）をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 dhcp server** を使用します。インターフェイスで IPv6 用 DHCP サービスをディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp server [*poolname*| **automatic**] **[rapid-commit]** [**preference** *value*] **[allow-hint]**

no ipv6 dhcp server

構文の説明

poolname	（任意）ローカルなプレフィックス プールのユーザ定義名。 プール名には象徴的な文字列（「Engineering」など）または整数（0 など）を使用できます。
automatic	（任意）サーバが、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。
rapid-commit	（任意）プレフィックス委任用に 2 メッセージ交換方式を許可します。
preference *value*	（任意）サーバにより送信されるアドバタイズ メッセージのプリファレンス オプションで伝送されるプリファレンス値を指定します。有効な範囲は 0 ～ 255 です。 プリファレンス値のデフォルトは 0 です。
allow-hint	（任意）サーバがクライアントによって提示されたプレフィックスの委任を考慮するかどうかを指定します。デフォルトでは、サーバはクライアントが提示したプレフィックスを無視します。

コマンド デフォルト

インターフェイスで IPv6 サービス用の DHCP はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.3(4)T	このコマンドが導入されました。
12.2(18)SXE	このコマンドが、Cisco IOS Release 12.2(18)SXE に統合されました。
12.4(24)T	**automatic** キーワードが追加されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
12.2(33)XNE	このコマンドが、Cisco IOS Release 12.2(33)XNE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 dhcp server コマンドは、指定されたインターフェイスを介してプレフィックス委任のプールおよびその他の設定を使用し、そのインターフェイスで IPv6 サービス用の DHCP をイネーブルにします。

automatic キーワードは、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。 サーバが IPv6 DHCP パケットを受信すると、サーバはそのパケットを DHCP リレーから受信したか、クライアントから直接受信したかを判別します。 リレーからパケットを受信した場合、サーバは、クライアントに最も近い最初のリレーと関連付けられているパケット内部のリンク アドレス フィールドを確認します。 サーバは、このリンク アドレスと、すべてのアドレス プレフィックスおよび IPv6 DHCP プールのリンク アドレス設定とを照合して、最長のプレフィックス一致を探します。 サーバは最長一致と関連付けられているプールを選択します。

パケットをクライアントから直接受信した場合、サーバは同じ照合を行いますが、照合を行うときに着信インターフェイスに設定されているすべての IPv6 アドレスを使用します。 そして再度、サーバは最長のプレフィックス照合を選択します。

rapid-commit キーワードは、プレフィックス委任およびその他の設定について、2 メッセージ交換を使用できるようにします。 クライアントが送信請求メッセージに高速コミット オプションを含め、サーバで **rapid-commit** キーワードがイネーブルになっている場合、サーバは応答メッセージを使用して送信請求メッセージに応答します。

preference キーワードを 0 以外の値とともに設定すると、サーバはプリファレンス オプションを追加して、アドバタイズ メッセージのプリファレンス値を伝送します。 この動作は、クライアントによるサーバの選択に影響を与えます。 プリファレンス オプションを含まないアドバタイズ

メッセージのプリファレンス値は 0 であると見なされます。 クライアントが 255 のプリファレンス値を持つプリファレンスオプションを含むアドバタイズメッセージを受信した場合、クライアントはアドバタイズ メッセージの送信元であるサーバに要求メッセージをすぐに送信します。

allow-hint キーワードを指定した場合、サーバは送信請求メッセージおよび要求メッセージに含まれる有効なクライアント提案のプレフィックスを委任します。 プレフィックスは、関連付けられているローカルプレフィックスプール内にあり、デバイスに割り当てられていない場合は有効です。 **allow-hint** キーワードを指定しない場合、提案は無視され、プレフィックスはプールの空きリストから委任されます。

IPv6 用 DHCP クライアント、サーバ、およびリレーの機能は、インターフェイス上で相互排他的です。 これらの機能のいずれかがすでにイネーブルになっていて、同じインターフェイスで別の機能を設定しようとすると、次のメッセージのいずれかが表示されます。

```
Interface is in DHCP client mode
Interface is in DHCP server mode
Interface is in DHCP relay mode
```

例

次に、server1 という名前のローカル プレフィックス プールに対して IPv6 用 DHCP をイネーブルにする例を示します。

```
Router(config-if)# ipv6 dhcp server server1
```

関連コマンド

コマンド	説明
ipv6 dhcp pool	IPv6 用 DHCP プールを設定し、IPv6 用 DHCP プール コンフィギュレーション モードを開始します。
show ipv6 dhcp interface	IPv6 用 DHCP のインターフェイス情報を表示します。

ipv6 enable

明示的な IPv6 アドレスが設定されていないインターフェイス上で IPv6 処理をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 enable** コマンドを使用します。明示的な IPv6 アドレスでまだ設定されていないインターフェイスで IPv6 処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 enable

no ipv6 enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IPv6 はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。
15.2(2)SNG	このコマンドが、Cisco ASR 901 シリーズのアグリゲーション サービス デバイスに実装されました。

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 enable コマンドは、インターフェイスに IPv6 リンクローカル ユニキャスト アドレスを自動的に設定し、さらにインターフェイスを IPv6 処理用にイネーブルにします。 明示的な IPv6 アドレスで設定されているインターフェイスで no **ipv6 enable** コマンドを実行しても、IPv6 処理はディセーブルになりません。

例

次に、イーサネット インターフェイス 0/0 で IPv6 処理をイネーブルにする例を示します。

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 enable
```

関連コマンド

コマンド	説明
ipv6 address link-local	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ipv6 address eui-64	IPv6 アドレスを設定して、そのアドレスの下位 64 ビットの EUI-64 インターフェイス ID を使用して、インターフェイスでの IPv6 処理をイネーブルにします。
ipv6 unnumbered	インターフェイスに明示的な IPv6 アドレスを割り当てなくても、インターフェイスで IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 host

ホスト名キャッシュにスタティックなホスト名/アドレスマッピングを定義するには、グローバル コンフィギュレーション モードで **ipv6 host** コマンドを使用します。 ホスト名/アドレス マッピングを削除するには、このコマンドの no 形式を使用します。

ipv6 host *name* [*port*] *ipv6-address*

no ipv6 host *name*

構文の説明

name	IPv6 ホストの名前。 名前の冒頭は、文字と数字のいずれも使用できます。 数字を使用すると、実行できるアクションは限られます。
port	（任意）対応付けられる IPv6 アドレスのデフォルト Telnet ポート番号。
ipv6-address	対応付けられる IPv6 アドレス。 ホスト名 1 つに最大 4 つのアドレスをバインドできます。

コマンド デフォルト

ホスト名キャッシュにスタティックなホスト名/アドレス マッピングは定義されていません。 デフォルトの Telnet ポートは 23 です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。

リリース	変更内容
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

*name*変数の先頭には、文字または数字を指定できます。 数字を使用すると、実行できる操作（**ping** など）が制限されます。

例

次の例では、2 つのスタティック マッピングを定義します。

```
Device(config)# ipv6 host cisco-sj 2001:0DB8:1::12
Device(config)# ipv6 host cisco-hq 2002:C01F:768::1 2001:0DB8:1::12
```

関連コマンド

コマンド	説明
show hosts	デフォルトのドメイン名、名前ルックアップ サービス、ネーム サーバ ホストのリスト、およびホスト名とアドレスのキャッシュされたリストを表示します。

ipv6 icmp error-interval

IPv6 インターネット制御メッセージ プロトコル（ICMP）エラー メッセージの間隔およびバケット サイズを設定するには、グローバル コンフィギュレーション モードで **ipv6 icmp error-interval** コマンドを使用します。 間隔をそのデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ipv6 icmp error-interval *milliseconds* [*bucketsize*]

no ipv6 icmp error-interval

構文の説明

milliseconds	バケットにトークンが保存される間隔。 許容範囲は 0 ～ 2147483647 です。デフォルトは 100 ミリ秒です。
bucketsize	（任意）バケットに保存されるトークンの最大数。 許容範囲は 1 ～ 200 です。デフォルトは 10 トークンです。

コマンド デフォルト

デフォルトでは、ICMP レート制限はイネーブルです。 ICMP レート制限をディセーブルにするには、間隔をゼロに設定します。 バケットにトークンが保存される間隔は 100 ミリ秒です。 バケットに保存されるトークンの最大数は 10 です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.2(8)T	IPv6 ICMP レート制限のサポートが、トークン バケットを使用するように拡張されました。
12.0(21)ST	トークン バケットを使用する拡張なしのこのコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	トークン バケットを使用する拡張なしのこのコマンドが Cisco IOS Release 12.0(22)S に統合されました。

リリース	変更内容
12.0(23)S	トークン バケットを使用するように拡張された IPv6 ICMP レート制限をサポートするこのコマンドが、Cisco IOS Release 12.0(23)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。
15.2(2)SNG	このコマンドが、Cisco ASR 901 シリーズのアグリゲーション サービス デバイスに実装されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

IPv6 ICMP エラー メッセージが送信されるレートを制限するには、**ipv6 icmp error-interval** コマンドを使用します。 トークン バケット アルゴリズムは、1 件の IPv6 ICMP エラー メッセージを表す 1 つのトークンで使用されます。 トークンは、バケットで許可されているトークンの最大数に達するまで、指定された間隔で、仮想バケットに保存されます。

milliseconds 引数は、トークンがバケットに到達する間隔を指定します。 オプションの *bucketsize* 引数は、バケットで許可されるトークンの最大数の定義に使用されます。 トークンは、IPv6 ICMP エラー メッセージが送信されるときにバケットから削除されます。つまり、*bucketsize* が 20 に設定されている場合、20 の IPv6 ICMP エラー メッセージを連続して送信することができます。 トークンのバケットが空になると、新しいトークンがバケットに配置されるまで、IPv6 ICMP エラー メッセージは送信されません。

show ipv6 traffic コマンドを使用すると、IPv6 ICMP レート制限カウンタを表示できます。

例

次の例は、50 ミリ秒の間隔と 20 トークンのバケット サイズが IPv6 ICMP エラー メッセージに対して設定されていることを示します。

```
ipv6 icmp error-interval 50 20
```

関連コマンド

コマンド	説明
show ipv6 traffic	IPv6 トラフィックに関する統計情報を表示します。

ipv6 nd cache expire

IPv6 ネイバー探索（ND）のキャッシュ エントリの期限が切れるまでの時間を設定するには、**ipv6 nd cache expire** コマンドをインターフェイス コンフィギュレーション モードで使用します。 このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

ipv6 nd cache expire *expire-time-in-seconds* **[refresh]**

no ipv6 nd cache expire *expire-time-in-seconds* **[refresh]**

構文の説明

expire-time-in-seconds	時間の範囲は 1 ～ 65536 秒です。 デフォルトは 14400 秒、つまり 4 時間です。
refresh	（任意）自動的に ND キャッシュ エントリをリフレッシュします。

コマンド デフォルト

この有効期限は 14400 秒（4 時間）です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI7	このコマンドが導入されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

デフォルトでは、ND キャッシュ エントリが 14,400 秒間（4 時間）、STALE 状態になると、期限切れとなり削除されます。 **ipv6 nd cache expire** コマンドは、エントリが削除される前にユーザが有効期限を変更して、期限切れのエントリの自動更新をトリガーできるようにします。

refresh キーワードを使用すると、ND キャッシュ エントリは自動更新されます。 エントリが DELAY 状態になり、ネイバー到達不能検出（NUD）プロセスが発生し、5 秒後に DELAY 状態から PROBE 状態にエントリが遷移します。 エントリが PROBE 状態になると、設定に従ってネイバー送信要求（NS）が送信され、再送信されます。

例

次に、ND キャッシュ エントリが 7200 秒（2 時間）で期限切れになるように設定する例を示します。

```
Router(config-if)# ipv6 nd cache expire 7200
```

ipv6 nd inspection

ネイバー探索プロトコル（NDP）チェック機能を適用するには、インターフェイス コンフィギュレーション モードで **ipv6 nd inspection** コマンドを使用します。 NDP インスペクション機能を削除するには、このコマンドの **no** 形式を使用します。

ipv6 nd inspection [**attach-policy** [*policy-name*] | **vlan** {**add** | **except** | **none** | **remove** | **all**} **vlan** *vlan-id*]]

no ipv6 nd inspection

構文の説明

attach-policy	（任意）NDP インスペクション ポリシーを適用します。
policy-name	（任意）NDP インスペクション ポリシー名。
vlan	（任意）インターフェイスの VLAN に ND インスペクション機能を適用します。
add	（任意）検査される VLAN を追加します。
except	（任意）指定した 1 つ以外のすべての VLAN を検査します。
none	（任意）VLAN を検査しないように指定します。
remove	（任意）NDP インスペクションから特定の VLAN を削除します。
all	（任意）ポートのすべての VLAN からの NDP トラフィックを検査します。
vlan-id	（任意）インターフェイスの特定の VLAN。 複数の VLAN を指定できます。 使用できる VLAN 番号は 1 ～ 4094 です。

コマンド デフォルト

すべての NDP メッセージが検査されます。 セキュア ネイバー探索（SeND）オプションは無視されます。 ネイバーはネイバー トラッキング機能で定義された基準に基づいて検査されます。 ポート単位の IPv6 アドレス制限の適用はディセーブルです。 レイヤ 2 ヘッダーの送信元 MAC アドレ

ス検証はディセーブルです。ソフトウェアでのNDPメッセージのポート単位のレート制限はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SY に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 nd inspection コマンドは、指定されたインターフェイスの NDP インスペクション機能を適用します。オプションの **attach-policy** または **vlan** キーワードをイネーブルにすると、NDP トラフィックがポリシーまたはVLANによって検査されます。VLANを指定しない場合は、ポートのすべての VLAN からの NDP のトラフィックが検査されます（**vlan all** キーワードを使用した場合と同じ）。

ポリシーがこのコマンドで指定されていない場合、デフォルトの条件は次のとおりです。

- すべての NDP メッセージが検査されます。
- SeND オプションは無視されます。
- ネイバーはネイバー トラッキング機能で定義された基準に基づいて検査されます。
- ポート単位の IPv6 アドレス制限の適用はディセーブルです。
- レイヤ 2 ヘッダーの送信元 MAC アドレス検証はディセーブルです。
- ソフトウェアでの NDP メッセージのポート単位のレート制限はディセーブルです。

VLAN を指定する場合、パラメータは、1 ～ 4094 の単一の VLAN 番号、または 2 つの VLAN 番号の小さい方を先にして、ダッシュで区切って記述した VLAN 範囲です（**vlan 1-100,200,300-400** など）。カンマで区切ったVLANパラメータの間、またはダッシュで指定した範囲の間には、スペースを入れないでください。

例

次に、指定されたインターフェイスのNDPインスペクションをイネーブルにする例を示します。

```
Router(config-if)# ipv6 nd inspection
```

ipv6 nd inspection policy

ネイバー探索（ND）インスペクション ポリシー名を定義して、ND インスペクション ポリシー コンフィギュレーション モードを開始するには、ND インスペクション コンフィギュレーション モードで **ipv6 nd inspection** コマンドを使用します。 ND インスペクション ポリシーを削除するには、このコマンドの **no** 形式を使用します。

ipv6 nd inspection policy *policy-name*

no ipv6 nd inspection policy *policy-name*

構文の説明

policy-name	ND インスペクション ポリシー名。

コマンド デフォルト

ND インスペクション ポリシーは設定されていません。

コマンド モード

ND インスペクション コンフィギュレーション（config-nd-inspection）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 nd inspection policy コマンドは、ND インスペクション ポリシー名を定義し、ND インスペクション ポリシー コンフィギュレーション モードを開始します。 ND インスペクション ポリシー コンフィギュレーション モードでは、次のコマンドのいずれかを使用できます。

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**

- **tracking**
- **trusted-port**
- **validate source-mac**

例

次に、policy1 として ND ポリシー名を定義する例を示します。

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)#
```

関連コマンド

コマンド	説明
device-role	ポートに接続されているデバイスのロールを指定します。
drop-unsecure	オプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをドロップします。
limit address-count	ポートで使用できる IPv6 アドレスの数を制限します。
sec-level minimum	CGA オプションを使用する場合の最小のセキュリティ レベル パラメータ値を指定します。
tracking	ポートでデフォルトのトラッキング ポリシーを上書きします。
trusted-port	信頼できるポートにするポートを設定します。
validate source-mac	リンク層アドレスと比較して送信元 MAC アドレスを検査します。

ipv6 nd na glean

ネイバー探索（ND）を設定し、非送信請求ネイバー アドバタイズメント（NA）からエントリを取り出すには、インターフェイス コンフィギュレーション モードで **ipv6 nd na glean** コマンドを使用します。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 nd na glean

no ipv6 nd na glean

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ルータは、非送信請求 NA を無視します。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI7	このコマンドが導入されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

IPv6 ノードは、重複アドレス検出（DAD）が正常に完了すると、マルチキャスト非送信請求 NA パケットを発行する場合があります。 デフォルトでは、これらの非送信請求 NA パケットは他の IPv6 ノードによって無視されます。 **ipv6 nd na glean** コマンドは、ルータを非送信請求 NA パケットの受信時にNDエントリを作成するように設定します（これらのエントリが存在せず、NAにリンク層アドレス オプションがあるものとします）。 このコマンドを使用すると、ルータがネイバーに対するデータ トラフィック交換の前にネイバーのエントリを ND キャッシュに読み込むことができます。

例

次に、非送信請求ネイバー アドバタイズメントからエントリを取り出すように ND を設定する例を示します。

```
Router(config-if)# ipv6 nd na glean
```

ipv6 nd nud retry

ネイバー到達不能検出（NUD）がネイバー送信要求（NS）を再送信する回数を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd nud retry** コマンドを使用します。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 nd nud retry *base interval max-attempts*

no ipv6 nd nud retry *base interval max-attempts*

構文の説明

base	ベース NUD 値。
interval	再試行の時間間隔（ミリ秒単位）。
max-attempts	再試行の最大数。base 値に依存します。

コマンド デフォルト

1 秒間隔で 3 回、NS パケットが送信されます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI7	このコマンドが導入されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ルータがネイバーの ND エントリを再解決するために NUD を実行するときに、1 秒間隔で 3 回、NS パケットを送信します。 特定の状況（スパニングツリー イベント、トラフィックが多い、エンド ホストがリロードされたなど）では、1 秒間隔で 3 回 NS パケットが送信されても十分でない場合があります。 こうした状況でネイバー キャッシュを維持するために、NS の再送信の指数タイマーを設定するには、**ipv6 nd nud retry** コマンドを使用します。

最大リトライ試行回数は *max-attempts* 引数を使用して設定します。 再送信間隔は、次の式を使用して計算されます。

tm

• *t* = 時間間隔

• *m* = ベース（1、2、または 3）

• *n* = 現在の NS の数（最初の NS が 0 に相当します）

ipv6 nd nud retry コマンドは、NUD の再送信のレートにのみ影響し、1 秒間隔で 3 回の NS パケット送信というデフォルトを使用する最初の解決には影響しません。

例

次に、1 秒間隔固定で 3 回再送信する例を示します。

```
Router(config-if)# ipv6 nd nud retry 1 1000 3
```

次に、1、2、4、8 の間隔で再送信する例を示します。

```
Router(config-if)# ipv6 nd nud retry 2 1000 4
```

次に、1、3、9、27、81 の間隔で再送信する例を示します。

```
Router(config-if)# ipv6 nd nud retry 3 1000 5
```

ipv6 nd ra-throttle attach-policy

レイヤ2インターフェイスまたはVLANのコレクションにIPv6ルータアドバタイズメント（RA）スロットル ポリシーを適用するには、インターフェイス コンフィギュレーション モードまたはVLAN コンフィギュレーション モードで **ipv6 nd ra-throttle attach-policy** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

ipv6 nd ra-throttle attach-policy *policy-name*

構文の説明

policy-name	RA スロットル ポリシー名。

コマンド デフォルト

ポリシーはインターフェイスに適用されません。

ポリシーは VLAN に適用されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

VLAN コンフィギュレーション（config-VLAN-config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

デバイス ポートのレイヤ2インターフェイスにIPv6 RA スロットル ポリシーを適用するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ra-throttle attach-policy** コマンドを使用します。 VLANまたはVLANのコレクションにIPv6 RA スロットル ポリシーを適用するには、VLAN コンフィギュレーション モードで **ipv6 nd ra-throttle attach-policy** コマンドを使用します。RA スロットル ポリシーを作成するには、グローバル コンフィギュレーション モードで **ipv6 nd ra-throttle policy** コマンドを使用します。

IPv6 RA スロットル ポリシーは、ポート レベルで動作させるために、VLAN またはボックス レベルで適用する必要があります。 ポリシーがポート レベルだけで適用されている場合、IPv6 RA スロットルは動作しません。

ポリシーがポートに適用されると、ポリシーで設定されていない値は VLAN 設定から継承されます。 値が VLAN 設定で設定されていない場合、デフォルト値が使用されます。

例

次に、policy1 という名前の IPv6 RA スロットル ポリシーを作成してイーサネット 0/0 インターフェイスに適用する例を示します。

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# exit
.
.
Device(config)# interface ethernet0/0
Device(config-if)# ipv6 nd ra-throttle attach-policy policy1
```

次に、policy1 という名前の IPv6 RA スロットル ポリシーを作成して vlan1 という名前の VLAN のコレクションに適用する例を示します。

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# exit
.
.
Device(config)# vlan configuration vlan1
Device(config-vlan-config)# ipv6 nd ra-throttle attach-policy policy1
```

ipv6 nd ra-throttle policy

ルータアドバタイズメント（RA）スロットルポリシー名を定義し、IPv6 RA スロットルポリシー コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **ipv6 nd ra-throttle policy** コマンドを使用します。 コマンドをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

ipv6 nd ra-throttle policy *policy-name* **no ipv6 nd ra-throttle policy** *policy-name*

構文の説明

policy-name	RA スロットル ポリシー名。

コマンド デフォルト

- throttle-period：600 秒（10 分）
- max-through：10 分あたり VLAN あたり 10 RA
- allow：少なくとも 1、最大 1
- interval-option：パススルー
- medium-type：有線（ポートのみ）

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

IPv6 RA スロットル ポリシーを定義し、IPv6 RA スロットル ポリシー コンフィギュレーション モードを開始するには、**ipv6 nd ra-throttle policy** コマンドを使用します。

VLAN レベルで適用される **allow at-least** および **allow at-most** コマンド設定は、VLAN 内のすべてのデバイスのデフォルトを指定します。 値は、指定されたポートに別のポリシーを適用することによって、ポート単位で上書きできます。

IPv6 RA スロットル ポリシーは、ポート レベルで動作させるために、VLAN またはボックス レベルで適用する必要があります。 ポリシーがポート レベルだけで適用されている場合、IPv6 RA スロットルは動作しません。

ポリシーがポートに適用されると、ポリシーで設定されていない値はVLAN設定から継承されます。 値がVLAN設定で設定されていない場合、デフォルト値が使用されます。

例

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)#
```

ipv6 nd raguard attach-policy

指定したインターフェイスにIPv6ルータアドバタイズメント（RA）ガード機能を適用するには、インターフェイス コンフィギュレーション モードで **ipv6 nd raguard attach-policy** コマンドを使用します。

ipv6 nd raguard attach-policy [*policy-name* [**vlan** {**add**| **except**| **none**| **remove**| **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]

構文の説明

policy-name	（任意）IPv6 RA ガード ポリシー名。
vlan	（任意）インターフェイスの VLAN に IPv6 RA ガード機能を適用します。
add	検査する VLAN を追加します。
except	指定した 1 つ以外のすべての VLAN を検査します。
none	VLAN は検査されません。
remove	RA ガード インスペクションから特定の VLAN を削除します。
all	ポートのすべての VLAN からの ND のトラフィックが検査されます。
vlan	（任意）インターフェイスの特定の VLAN。 複数の VLAN を指定できます（*vlan1*, *tb-vlan2*, *vlan3...*）。 使用できる VLAN 番号の範囲は 1 ～ 4094 です。

コマンド デフォルト

IPv6 RA ガード ポリシーは設定されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.2(4)S	このコマンドが Cisco IOS Release 15.2(4)S に統合されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

policy-name 引数を使用してポリシーが指定されない場合、ポートデバイス ロールはホストに設定され、すべてのインバウンド ルータ トラフィック（RA メッセージ、リダイレクト メッセージなど）がブロックされます。

VLAN が指定されない場合（**vlan all** キーワードを *policy-name* 引数に続けて入力した場合と同じ）、ポートのすべての VLAN からの RA ガード トラフィックが解析されます。

VLAN パラメータは、1 ～ 4094 の間の 1 つの VLAN 番号、または 2 つの VLAN 番号で指定する（小さい方の数を先にして、間をダッシュで区切る）VLAN 範囲です。 カンマで区切った vlan パラメータの間、またはダッシュで指定した範囲の間には、スペースを入れないでください（例：vlan 1-100,200,300-400）。

例

次の例では、IPv6 RA ガード機能が GigabitEthernet インターフェイス 0/0 に適用されます。

```
Device(config)# interface GigabitEthernet 0/0
Device(config-if)# ipv6 nd raguard attach-policy
```

ipv6 nd raguard policy

ルータアドバタイズメント（RA）ガードポリシー名を定義し、RAガードポリシーコンフィギュレーションモードを開始するには、グローバルコンフィギュレーションモードで**ipv6 nd raguard policy** コマンドを使用します。

ipv6 nd raguardpolicy *policy-name*

構文の説明

policy-name	IPv6 RA ガード ポリシー名。

コマンド デフォルト

RA ガード ポリシーは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.2(4)S	このコマンドが Cisco IOS Release 15.2(4)S に統合されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ルータでRAガードをグローバルに設定するには、**ipv6 nd raguard policy** コマンドを使用します。デバイスがNDインスペクションポリシーコンフィギュレーションモードの場合、次のコマンドのいずれかを使用できます。

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**
- **trusted-port**

- **validate source-mac**

IPv6 RA ガードをグローバルに設定した後、**ipv6 nd raguard attach-policy** コマンドを使用して、特定のインターフェイスで IPv6 RA ガードをイネーブルにできます。

例

次に、policy1 という RA ガード ポリシー名を定義し、デバイスをポリシー コンフィギュレーション モードにする例を示します。

```
Device(config)# ipv6 nd raguard policy policy1
Device(config-ra-guard)#
```

関連コマンド

コマンド	説明
device-role	ポートに接続されているデバイスのロールを指定します。
drop-unsecure	オプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをドロップします。
ipv6 nd raguard attach-policy	指定したインターフェイスで IPv6 RA ガード機能を適用します。
limit address-count	ポートで使用できる IPv6 アドレスの数を制限します。
sec-level minimum	CGA オプションを使用する場合の最小のセキュリティ レベル パラメータ値を指定します。
trusted-port	信頼できるポートにするポートを設定します。
validate source-mac	リンク層アドレスと比較して送信元 MAC アドレスを検査します。

ipv6 nd router-preference

特定のインターフェイス上のルータにデフォルト ルータ プリファレンス（DRP）を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd router-preference** コマンドを使用します。 デフォルト DRP に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd router-preference {**high**| **medium**| **low**}

no ipv6 nd router-preference

構文の説明

high	インターフェイスで指定されたルータの優先順位は高です。
medium	インターフェイスで指定されたルータの優先順位は中です。
low	インターフェイスで指定されたルータの優先順位は低です。

コマンド デフォルト

ルータ アドバタイズメント（RA）は、**medium** プリファレンスとともに送信されます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.4(2)T	このコマンドが導入されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.2(33)SB	このコマンドが、Cisco IOS Release 12.2(33)SB に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

RA メッセージは、**ipv6 nd router-preference** コマンドで設定された DRP とともに送信されます。DRP が設定されていない場合は、RA は中小規模のプリファレンスとともに送信されます。

DRP は、リンク上の 2 台のルータが、同等だがコストが等しくないルーティングを提供するときに、ホストがいずれかのルータを優先するようにポリシーで指示する場合に役立ちます。

例

次に、ギガビット イーサネット インターフェイス 0/1 上のルータに高い DRP を設定する例を示します。

```
Router(config)# interface Gigabit ethernet 0/1
Router(config-if)# ipv6 nd router-preference high
```

関連コマンド

コマンド	説明
ipv6 nd ra interval	インターフェイスで IPv6 ルータ アドバタイズメント メッセージが送信される時間間隔を設定します。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd suppress attach-policy

指定したインターフェイスに IPv6 ネイバー探索（ND）抑制機能を適用するには、インターフェイス コンフィギュレーション モードで **ipv6 nd suppress attach-policy** コマンドを使用します。

ipv6 nd suppress attach-policy [*policy-name* [**vlan** {**add| except| none| remove| all**} *vlan* [*vlan1, vlan2, vlan3...*]]]

構文の説明

policy-name	（任意）IPv6 ND 抑制ポリシー名。
vlan	（任意）インターフェイスの VLAN に IPv6 ND 抑制機能を適用します。
add	検査する VLAN を追加します。
except	指定した 1 つ以外のすべての VLAN を検査します。
none	VLAN は検査されません。
remove	IPv6 ND 抑制から特定の VLAN を削除します。
all	ポートのすべての VLAN からの ND のトラフィックが検査されます。
vlan	（任意）インターフェイスの特定の VLAN。 複数の VLAN を指定できます（*vlan1*, *tb-vlan2*, *vlan3...*）。 使用できる VLAN 番号の範囲は 1 ～ 4094 です。

コマンド デフォルト

IPv6 ND 抑制ポリシーは設定されていません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
15.3(1)S	このコマンドが導入されました。

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

VLAN が指定されない場合（**vlan all** キーワードを *policy-name* 引数に続けて入力した場合と同じ）、ポートのすべての VLAN からの RA ガード トラフィックが解析されます。

VLAN パラメータは、1 ～ 4094 の間の 1 つの VLAN 番号、または 2 つの VLAN 番号で指定する（小さい方の数を先にして、間をダッシュで区切る）VLAN 範囲です。 カンマで区切った vlan パラメータの間、またはダッシュで指定した範囲の間には、スペースを入れないでください（例：vlan 1-100,200,300-400）。

例

次の例では、IPv6 ND 抑制機能がイーサネット インターフェイス 0/0 に適用されます。

```
Device(config)# interface Ethernet 0/0
Device(config-if)# ipv6 nd suppress attach-policy
```

関連コマンド

コマンド	説明
ipv6 nd suppress policy	IPv6 ND マルチキャスト抑制をイネーブルにして、ND 抑制ポリシー コンフィギュレーション モードを開始します。

ipv6 nd suppress policy

IPv6 ネイバー探索（ND）マルチキャスト抑制をイネーブルにして、ND 抑制ポリシー コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **ipv6 nd suppress policy** コマンドを使用します。

ipv6 nd suppress policy *policy-name*

構文の説明

policy-name	IPv6 ND 抑制ポリシー名。

コマンド デフォルト

ND 抑制ポリシーは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
15.3(1)S	このコマンドが導入されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

デバイスの NA 抑制をグローバルに設定するには、**ipv6 nd suppress policy** コマンドを使用します。IPv6 ND 抑制をグローバルに設定した後、**ipv6 nd suppress attach-policy** コマンドを使用して、特定のインターフェイスで IPv6 ND 抑制をイネーブルにできます。

例

次に、policy1 という ND 抑制ポリシー名を定義し、デバイスをポリシー コンフィギュレーション モードにする例を示します。

```
Device(config)# ipv6 nd suppress policy policy1
Device(config-nd-suppress)#
```

関連コマンド

コマンド	説明
ipv6 nd suppress attach-policy	指定したインターフェイスで IPv6 ND 抑制機能を適用します。

ipv6 neighbor binding logging

バインディング テーブルの主要イベントのロギングをイネーブルにするには、グローバル コンフィギュレーション モードで **ipv6 neighbor binding logging** コマンドを使用します。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 neighbor binding logging

no ipv6 neighbor binding logging

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

バインディング テーブルのイベントはログに記録されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 neighbor binding logging コマンドによって、次のようなバインディング テーブルのイベントをロギングできます。

- エントリがバインディング テーブルに挿入される。
- バインディング テーブル エントリが更新された。
- バインディング テーブル エントリがバインディング テーブルから削除された。
- バインディング テーブル エントリが既存エントリと衝突するため、またはエントリの最大数に到達したため、バインディング テーブルに挿入されなかった。

例

次に、バインディング テーブルのイベントのロギングをイネーブルにする例を示します。

```
Router(config)# ipv6 neighbor binding logging
```

関連コマンド

コマンド	説明
ipv6 neighbor binding vlan	バインディング テーブル データベースにスタティック エントリを追加します。
ipv6 neighbor tracking	バインディングテーブルのエントリを追跡します。
ipv6 snooping logging packet drop	IPv6 スヌーピング セキュリティのロギングを設定します。

ipv6 neighbor binding max-entries

バインディングテーブルキャッシュに挿入できるエントリの最大数を指定するには、グローバル コンフィギュレーション モードで **ipv6 neighbor binding max-entries** コマンドを使用します。 デフォルトに戻るには、**no** 形式のコマンドを使用します。

ipv6 neighbor binding max-entries *entries* [**vlan-limit** *number*| **interface-limit** *number*| **mac-limit** *number*]

no ipv6 neighbor binding max-entries *entries* [**vlan-limit**| **mac-limit**]

構文の説明

entries	キャッシュに挿入できるエントリ数。
vlan-limit *number*	（任意）VLAN数ごとにネイバーバインディング制限を指定します。
interface-limit *number*	（任意）インターフェイスごとにネイバーバインディング制限を指定します。
mac-limit *number*	（任意）メディア アクセス コントロール（MAC）アドレスごとにネイバー バインディング制限を指定します。

コマンド デフォルト

このコマンドはディセーブルです。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 neighbor binding max-entries コマンドは、バインディング テーブルの内容を制御するために使用されます。 このコマンドは、バインディング テーブル キャッシュに挿入できるエントリの最大数を指定します。 この制限に到達すると、新しいエントリは拒否され、新しいエントリとネイバー探索プロトコル（NDP）トラフィックの送信元はドロップされます。

指定できるエントリの最大数がデータベース内の現在のエントリ数未満の場合、エントリはクリアされず、通常のキャッシュ削減後に新しいしきい値に到達します。

エントリの最大数は VLAN 数または MAC アドレス数によってグローバルに設定できます。

例

次に、キャッシュに挿入されるエントリの最大数をグローバルに指定する例を示します。

```
Router(config)# ipv6 neighbor binding max-entries 100
```

関連コマンド

コマンド	説明
ipv6 neighbor binding vlan	バインディング テーブル データベースにスタティック エントリを追加します。
ipv6 neighbor tracking	バインディングテーブルのエントリを追跡します。

ipv6 neighbor binding vlan

バインディング テーブル データベースにスタティック エントリを追加するには、グローバル コンフィギュレーション モードで **ipv6 neighbor binding vlan** コマンドを使用します。 スタティック エントリを削除するには、このコマンドの **no** 形式を使用します。

ipv6 neighbor binding vlan *vlan-id* {**interface** *type number*| *ipv6-address*| *mac-address*} [**tracking** [**disable**| **enable**| **retry-interval** *value*]| **reachable-lifetime** *value*]

no ipv6 neighbor binding vlan *vlan-id*

構文の説明

vlan-id	指定した VLAN の ID。
interface *type number*	指定したインターフェイス タイプおよび番号でスタティック エントリを追加します。
ipv6-address	スタティック エントリの IPv6 アドレス。
mac-address	スタティック エントリのメディア アクセス コントロール（MAC）アドレス。
tracking	（任意）スタティック エントリの到達可能性を直接確認します。
disable	（任意）特定のスタティック エントリのトラッキングをディセーブルにします。
enable	（任意）特定のスタティック エントリのトラッキングをイネーブルにします。
retry-interval *value*	（任意）設定された間隔でスタティック エントリの到達可能性を秒単位で確認します。 指定できる範囲は 1 ～ 3600 で、デフォルトは 300 です。
reachable-lifetime *value*	（任意）到達可能という証明（トラッキングを介した直接的な到達可能、またはネイバー探索プロトコル（NDP）インスペクションを介した間接的な到達可能性）を受け取らずにエントリが到達可能と見なされる最大時間（秒単位）です。 その後、エントリは期限切れになります。 有効な範囲は 1 ～ 3600 秒で、デフォルトは 300 秒です。

コマンド デフォルト

再試行間隔：300 秒

到達可能ライフタイム：300 秒

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 neighbor binding vlan コマンドは、バインディング テーブルの内容を制御するために使用されます。 バインディング テーブル データベースにスタティック エントリを追加するには、このコマンドを使用します。バインディングテーブルマネージャがエントリをエージングアウトし、プローブして到達可能性を直接確認します（**tracking** キーワードがイネーブルの場合）。 **tracking** キーワードは、このスタティック エントリの **ipv6 neighbor tracking** コマンドによってグローバルに提供される一般的な動作をオーバーライドします。 **disable** キーワードは、このスタティック エントリのトラッキングをディセーブルにします。 **stale-lifetime** キーワードは、到達可能でない（または期限切れ）と判断してからエントリを保持する最大時間を定義します。

例

次に、バインディング エントリの到達可能ライフタイムを 100 秒に変更する例を示します。

```
Router(config)# ipv6 neighbor binding vlan reachable-lifetime 100
```

関連コマンド

コマンド	説明
ipv6 neighbor binding max-entries	キャッシュに挿入できるエントリの最大数を指定します。
ipv6 neighbor tracking	バインディングテーブルのエントリを追跡します。

ipv6 neighbor tracking

バインディング テーブルのエントリを追跡するには、グローバル コンフィギュレーション モードで **ipv6 neighbor tracking** コマンドを使用します。 エントリ追跡をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 neighbor tracking [**retry-interval** *value*]

no ipv6 neighbor tracking [**retry-interval** *value*]

構文の説明

retry-interval *value*	（任意）設定された間隔でスタティック エントリの到達可能性を確認します（秒単位）。2 回のプローブの間隔です。 指定できる範囲は1～3600 で、デフォルトは 300 です。

コマンド デフォルト

再試行間隔：300 秒

到達可能ライフタイム：300 秒

期限切れライフタイム：1440 分

ダウン ライフタイム：1440 分

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 neighbor tracking コマンドは、バインディング テーブルのエントリのトラッキングをイネーブルにします。 エントリの到達可能性は、ネイバー到達可能性の直接トラッキングに使用するネイバー到達不能検出（NUD）メカニズムを使用して、オプションの **retry-interval** キーワードで設定された間隔で（またはデフォルトの再試行間隔である 300 秒ごとに）テストされます。

到達可能性は、VERIFY_MAX_RETRIES 値（デフォルトは 10 秒）までネイバー探索プロトコル（NDP）インスペクションを使用して間接的に確立することもできます。 応答がない場合、エントリは期限切れライフタイム値に到達した後に期限切れと見なされ、削除されます（デフォルトは 1440 分）。

ipv6 neighbor tracking コマンドがディセーブルの場合、エントリは到達可能ライフタイム値（デフォルトは 300 秒）に達すると期限切れと見なされ、期限切れライフタイム値に達すると削除されます。

バインディング テーブルのネイバー バインディング エントリのデフォルト値を変更するには、**ipv6 neighbor binding** コマンドを使用します。

例

次に、バインディング テーブルのエントリを追跡する例を示します。

```
Router(config)# ipv6 neighbor tracking
```

関連コマンド

コマンド	説明
ipv6 neighbor binding	バインディングテーブルのネイバーバインディング エントリのデフォルトを変更します。

ipv6 prefix-list

IPv6プレフィックス リストのエントリを作成するには、グローバル コンフィギュレーション モードで **ipv6 prefix-list** コマンドを使用します。 エントリを削除するには、このコマンドの **no** 形式を使用します。

ipv6 prefix-list *list-name* [**seq** *seq-number*] {**deny** *ipv6-prefix*/*prefix-length*| **permit** *ipv6-prefix*/*prefix-length*| **description** *text*} [**ge** *ge-value*] [**le** *le-value*]

no ipv6 prefix-list *list-name*

構文の説明

list-name	プレフィックス リストの名前。 • 既存のアクセス リストと同じ名前にはできません。 • 「detail」または「summary」という名前にはできません。これらは、**show ipv6 prefix-list** コマンドのキーワードです。
seq *seq-number*	（任意）設定されるプレフィックス リスト エントリのシーケンス番号。
deny	基準を満たすネットワークを拒否します。
permit	基準を満たすネットワークを許可します。
ipv6-prefix	指定したプレフィックス リストに割り当てられる IPv6 ネットワーク。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの16ビット値を使用して、アドレスを 16 進数で指定します。
/*prefix-length*	IPv6 プレフィックスの長さ。 プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す10進値です。10 進数値の前にスラッシュ記号が必要です。
description *text*	プレフィックス リストの説明。長さは 80 文字までです。

ge *ge-value*	（任意）*ipv6-prefix*/*prefix-length* 引数と同じ、またはそれよりも長いプレフィックス長を指定します。 *length* の範囲の最小値です（長さの範囲の「から」の部分）。
le *le-value*	（任意）*ipv6-prefix*/*prefix-length* 引数と同じ、またはそれよりも短いプレフィックス長を指定します。 *length* の範囲の最大値です（長さの範囲の「まで」の部分）。

コマンド デフォルト　プレフィックス リストは作成されません。

コマンド モード　グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン　IPv6 固有である点を除くと、**ipv6 prefix-list** コマンドは **ip prefix-list** コマンドと類似しています。

ネットワークがアップデートでアドバタイズされないようにするには、**distribute-list out** コマンドを使用します。

プレフィックスリストエントリのシーケンス番号によって、リスト中のエントリの順番が決まります。 ルータは、ネットワーク アドレスとプレフィックス リスト エントリを比較します。 ルータは、プレフィックス リストの先頭（最も小さいシーケンス番号）から比較を開始します。

プレフィックス リストの複数のエントリがプレフィックスに一致する場合、シーケンス番号が最も小さいエントリが実際の一致と見なされます。 一致または拒否が発生すると、プレフィックス リストの残りのエントリは処理されません。 効率性のために、*seq-number* 引数を使用して、リストの上部に最も一般的な許可または拒否を配置できます。

show ipv6 prefix-list コマンドは、エントリのシーケンス番号を表示します。

IPv6 プレフィックス リストは、permit 文または deny 文を適用する前に照合が必要な特定のプレフィックスまたはプレフィックスの範囲を指定するために使用されます。 2 つのオペランド キーワードを使用して、照合するプレフィックス長の範囲を指定できます。 ある値以下のプレフィックス長は、**le** キーワードで設定します。 ある値以上のプレフィックス長は、**ge** キーワードを使用して指定します。 **ge** および **le** キーワードを使用すると、通常の *ipv6-prefix/prefix-length* 引数よりも詳細に、照合するプレフィックス長の範囲を指定できます。プレフィックス リストのエントリと照合される候補プレフィックスに対して、次の 3 つの条件が存在する可能性があります。

- 候補プレフィックスは、指定したプレフィックス リストおよびプレフィックス長エントリと一致している必要があります。
- 省略可能な **le** キーワードの値によって、許可されるプレフィックス長が、*prefix-length* 引数から **le** キーワードの値（この値を含む）までの範囲で指定されます。
- オプションの **ge** キーワードの値は、許可されるプレフィックス長の範囲を **ge** キーワードの値から最大 128 までに指定します（128 も含まれます）。

（注） 最初の条件は、他の条件が有効になる前に一致している必要があります。

ge または **le** キーワードを指定しなかった場合は、完全一致であると想定されます。 1 つのキーワード オペランドだけを指定した場合、そのキーワードの条件が適用され、もう 1 つの条件は適用されません。 *prefix-length* 値は、**ge** 値よりも小さい必要があります。 **ge** 値は、**le** 値以下である必要があります。 **le** 値は、128 以下である必要があります。

すべてのIPv6プレフィックスリスト（許可および拒否の条件文が含まれていないプレフィックス リストを含む）には、最後の一致条件として暗黙的な deny any any 文が含まれています。

例

次の例は、プレフィックス ::/0 のすべてのルートを拒否します。

```
Router(config)# ipv6 prefix-list abc deny ::/0
```

次に、プレフィックス 2002::/16 を許可する例を示します。

```
Router(config)# ipv6 prefix-list abc permit 2002::/16
```

次に、プレフィックス 5F00::/48 からプレフィックス 5F00::/64 までのすべてのプレフィックスを受け入れるようにプレフィックスのグループを指定する例を示します。

```
Router(config)# ipv6 prefix-list abc permit 5F00::/48 le 64
```

次の例は、プレフィックス 2001:0DB8::/64 のルートで 64 ビットを超えるプレフィックス長を拒否します。

```
Router(config)# ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
```

次の例は、すべてのアドレス空間で 32 ～ 64 ビットのマスク長を許可します。

```
Router(config)# ipv6 prefix-list abc permit ::/0 ge 32 le 64
```

次の例は、すべてのアドレス空間で 32 ビットを超えるマスク長を拒否します。

```
Router(config)# ipv6 prefix-list abc deny ::/0 ge 32
```

次の例は、プレフィックス 2002::/128 のすべてのルートを拒否します。

```
Router(config)# ipv6 prefix-list abc deny 2002::/128
```

次の例は、プレフィックス ::/0 のすべてのルートを許可します。

```
Router(config)# ipv6 prefix-list abc permit ::/0
```

関連コマンド

コマンド	説明
clear ipv6 prefix-list	IPv6 プレフィックス リスト エントリのヒット カウントをリセットします。
distribute-list out	ネットワークがアップデート時にアドバタイズされないようにします。
ipv6 prefix-list sequence-number	IPv6 プレフィックス リストのエントリのシーケンス番号の生成をイネーブルにします。
match ipv6 address	プレフィックス リストによって許可されるプレフィックスを持つ IPv6 ルートを配布します。
show ipv6 prefix-list	IPv6 プレフィックス リストまたは IPv6 プレフィックス リストのエントリに関する情報を表示します。

ipv6-i4

- ipv6 snooping attach-policy, 119 ページ
- ipv6 snooping policy, 121 ページ
- ipv6 traffic-filter, 123 ページ
- ipv6 verify unicast source reachable-via, 125 ページ
- managed-config-flag, 128 ページ
- match ipv6, 130 ページ
- match ipv6 access-list, 133 ページ
- match ipv6 address, 135 ページ
- match ipv6 destination, 139 ページ
- match ipv6 hop-limit, 142 ページ
- match ra prefix-list, 144 ページ
- max-through, 146 ページ
- medium-type, 147 ページ
- mode dad-proxy, 148 ページ
- network（IPv6）, 150 ページ
- other-config-flag, 152 ページ
- passive-interface（IPv6）, 154 ページ
- passive-interface（OSPFv3）, 156 ページ
- permit（IPv6）, 158 ページ
- prefix-glean, 171 ページ
- protocol（IPv6）, 173 ページ
- redistribute（IPv6）, 175 ページ

- router-preference maximum, 182 ページ

ipv6 snooping attach-policy

ターゲットに IPv6 スヌーピング ポリシーを適用するには、IPv6 スヌーピング コンフィギュレーション モードで **ipv6 snooping attach-policy** コマンドを使用します。 ターゲットからポリシーを削除するには、このコマンドの **no** 形式を使用します。

ipv6 snooping policy attach-policy *snooping-policy*

構文の説明

snooping-policy	スヌーピング ポリシーのユーザ定義名。 ポリシー名には象徴的な文字列（Engineering など）または整数（0 など）を使用できます。

コマンド デフォルト

IPv6 スヌーピング ポリシーは、ターゲットに適用されていません。

コマンド モード

IPv6 スヌーピング コンフィギュレーション（config-ipv6-snooping）

コマンド履歴

リリース	変更内容
15.0(2)SE	このコマンドが導入されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ポリシーを識別または設定した後、**ipv6 snooping attach-policy** コマンドを使用してターゲットに適用します。 このコマンドは、プラットフォームに応じて、任意のターゲットに適用されます。ターゲットの例（使用するプラットフォームによる）として、デバイス ポート、スイッチポート、レイヤ 2 インターフェイス、レイヤ 3 インターフェイス、VLAN があります。

例

次に、policy1 という名前の IPv6 スヌーピング ポリシーをターゲットに適用する例を示します。

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# ipv6 snooping attach-policy policy1
```

関連コマンド

コマンド	説明
ipv6 snooping policy	IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング コンフィギュレーション モードを開始します。

ipv6 snooping policy

IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **ipv6 snooping policy** コマンドを使用します。 IPv6 スヌーピング ポリシーを削除するには、このコマンドの **no** 形式を使用します。

ipv6 snooping policy *snooping-policy*

no ipv6 snooping policy *snooping-policy*

構文の説明

snooping-policy	スヌーピング ポリシーのユーザ定義名。 ポリシー名には象徴的な文字列（Engineering など）または整数（0 など）を使用できます。

コマンド デフォルト

IPv6 スヌーピング ポリシーは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
15.0(2)SE	このコマンドが導入されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 snooping policy コマンドを使用して、IPv6 スヌーピング ポリシーを作成できます。 **ipv6 snooping policy** コマンドをイネーブルにすると、コンフィギュレーション モードが IPv6 スヌーピング コンフィギュレーション モードに変わります。 このモードでは、管理者が次の IPv6 第 1 ホップ セキュリティ コマンドを設定できます。

- **data-glean/destination-glean** コマンドは、データまたは宛先アドレス グリーニングを使用した IPv6 第 1 ホップ セキュリティ バインディング テーブルのリカバリをイネーブルにします。
- **device-role** コマンドは、ポートに接続されたデバイスのロールを指定します。

- **limit address-count** *maximum* コマンドは、ポートで使用できる IPv6 アドレスの数を制限します。
- **security-level** は、適用されるセキュリティのレベルを指定します。
- **tracking** コマンドは、ポートのデフォルトのトラッキング ポリシーを上書きします。
- **trusted-port** コマンドは、信頼できるポートとしてポートを設定します。つまり、メッセージの受信時に検証が実行されないか、限られた検証だけが実行されます。

ポリシーを識別または設定した後、**ipv6 snooping attach-policy** コマンドを使用してデバイスに適用します。

例

次に、IPv6 スヌーピング ポリシーを設定する例を示します。

```
Device(config)# ipv6 snooping policy policy1
```

関連コマンド

コマンド	説明
ipv6 snooping attach-policy	ターゲットに IPv6 スヌーピングにポリシーを適用します。

ipv6 traffic-filter

インターフェイスで着信または発信 IPv6 トラフィックをフィルタリングするには、インターフェイス コンフィギュレーション モードで **ipv6 traffic-filter** コマンドを使用します。 インターフェイスで IPv6 トラフィックのフィルタリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 traffic-filter *access-list-name* {**in**| **out**}

no ipv6 traffic-filter *access-list-name*

構文の説明

access-list-name	IPv6 アクセス名を指定します。
in	着信 IPv6 トラフィックを指定します。
out	発信 IPv6 トラフィックを指定します。

コマンド デフォルト

インターフェイス上での IPv6 トラフィックのフィルタリングは設定されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ ルータで追加されました。
12.2(33)SXI4	**out** キーワード、すなわち発信トラフィックのフィルタリングは IPv6 ポート ベース アクセス リスト（PACL）設定ではサポートされません。
12.2(54)SG	このコマンドが変更されました。 Cisco IOS Release 12.2(54)SG のサポートが追加されました。
12.2(50)SY	このコマンドが変更されました。 **out** キーワードはサポートされません。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

例

次に、cisco という名前のアクセス リストの定義に従って、イーサネット インターフェイス 0/0 でインバウンド IPv6 トラフィックをフィルタリングする例を示します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 traffic-filter cisco in
```

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを定義し、定義されたアクセス リストに拒否または許可条件を設定します。
show ipv6 access-list	現在のすべての IPv6 アクセス リストの内容を表示します。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 verify unicast source reachable-via

送信元アドレスがFIBテーブルに存在し、ユニキャストリバースパス転送（ユニキャストRPF）がイネーブルであることを確認するには、インターフェイス コンフィギュレーション モードで **ipv6 verify unicast source reachable-via** コマンドを使用します。URPFをディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 verify unicast source reachable-via {**rx**| **any**} **[allow-default] [allow-self-ping]** [*access-list-name*]

no ipv6 verify unicast

構文の説明

rx	送信元は、パケットを受信したインターフェイスを通じて到達できます。
any	送信元は、どのインターフェイスからでも到達可能です。
allow-default	（任意）ルックアップ テーブルがデフォルトルートを照合し、確認のためにルートを使用できるようにします。
allow-self-ping	（任意）ルータがセカンダリアドレスへのpingを実行できるようにします。
access-list-name	（任意）IPv6アクセス リストの名前。名前にはスペースまたは引用符を含めることはできません。また、数字で始めることはできません。

コマンド デフォルト

ユニキャストRPFはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(25)S	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SBに統合されました。

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータで導入されました。

使用上のガイドライン

ipv6 verify unicast reverse-path コマンドは、ルーズ チェック モードで IPv6 のユニキャスト RPF をイネーブルにするために使用します。

ipv6 verify unicast source reachable-via コマンドは、IPv6 ルータをパススルーする不正形式または偽造（スプーフィング）IP送信元アドレスによって発生する問題を減少させるために使用します。不正形式または偽造送信元アドレスは、送信元IPv6アドレススプーフィングに基づくサービス拒絶（DoS）攻撃を示すことがあります。

URPF 機能は、ルータ インターフェイスで受信されるパケットが、パケットの送信元への最良リターンパスのいずれかで到達するかどうかを確認します。 これは、CEFテーブルの逆ルックアップを実行することによって行います。 URPF でパケットのリバース パスが見つからない場合、アクセス コントロール リスト（ACL）が **ipv6 verify unicast source reachable-via** コマンドで指定されているかどうかに応じて、URPF はパケットをドロップまたは転送できます。 コマンドで ACL を指定し、パケットがURPFの確認に失敗した場合にのみ、ACLを確認して（ACLでdenyステートメントを使用して）パケットをドロップするか、（ACLでpermitステートメントを使用して）転送するかを参照します。 パケットがドロップされるか転送されるかにかかわらず、パケットは、URPF ドロップのグローバル IP トラフィック統計情報とユニキャスト RPF のインターフェイス統計情報でカウントされます。

ipv6 verify unicast source reachable-via コマンドで ACL を指定しない場合、ルータは偽造または不正な形式のパケットをただちにドロップし、ACLのロギングは発生しません。 ルータおよびインターフェイス ユニキャスト RPF カウンタが更新されます。

URPF イベントをロギングするには、**ipv6 verify unicast source reachable-via** コマンドで使用する ACL エントリのロギング オプションを指定します。 ログ情報を使用して、送信元アドレスや時間など、攻撃に関する情報を収集できます。

例

次に、インターフェイスでユニキャスト RPF をイネーブルにする例を示します。

```
ipv6 verify unicast source reachable-via any
```

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを定義し、ルータを IPv6 アクセス リスト コンフィギュレーション モードにします。

コマンド	説明
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

managed-config-flag

アドバタイズされた管理対象アドレス設定パラメータを確認するには、RA ガード ポリシー コンフィギュレーション モードで **managed-config-flag** コマンドを使用します。

managed-config-flag {**on**| **off**}

構文の説明

on	検証はイネーブルです。
off	検証はディセーブルです。

コマンド デフォルト

検証はイネーブルになりません。

コマンド モード

RA ガード ポリシー コンフィギュレーション（config-ra-guard）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.2(4)S	このコマンドが Cisco IOS Release 15.2(4)S に統合されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

managed-config-flag コマンドによって、アドバタイズされた管理対象アドレス設定パラメータ（「M」フラグ）を検証できます。 このフラグは、信頼できない可能性がある DHCPv6 サーバを通じてホストにアドレスを取得させるために、攻撃者によって設定されることがあります。

例

次に、ルータ アドバタイズメント（RA）ガード ポリシー名を raguard1 として定義し、ルータを RA ガード ポリシー コンフィギュレーション モードにして、M フラグの検証をイネーブルにする例を示します。

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# managed-config-flag on
```

関連コマンド

コマンド	説明
ipv6 nd raguard policy	RA ガード ポリシー名を定義し、RA ガード ポリシー コンフィギュレーション モードを開始します。

match ipv6

フロー レコードのキー フィールドとして IPv6 フィールドの 1 つ以上を設定するには、Flexible NetFlow フロー レコード コンフィギュレーション モードで **match ipv6** コマンドを使用します。フロー レコードのキー フィールドとして IPv6 フィールドの 1 つ以上の使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv6 {**dscp**| **flow-label**| **next-header**| **payload-length**| **precedence**| **protocol**| **traffic-class**| **version**}

no match ipv6 {**dscp**| **flow-label**| **next-header**| **payload-length**| **precedence**| **protocol**| **traffic-class**| **version**}

Cisco Catalyst 6500 Switches in Cisco IOS Release 12.2(50)SY

match ipv6 {**dscp**| **precedence**| **protocol**| **tos**}

no match ipv6 {**dscp**| **precedence**| **protocol**| **tos**}

Cisco IOS XE Release 3.2SE

match ipv6 {**protocol**| **traffic-class**| **version**}

no match ipv6 {**protocol**| **traffic-class**| **version**}

構文の説明

dscp	キー フィールドとして IPv6 DiffServ コード ポイント DSCP（タイプ オブ サービス（ToS）の一部）を設定します。
flow-label	キー フィールドとして IPv6 フロー ラベルを設定します。
next-header	キー フィールドとして IPv6 次ヘッダーを設定します。
payload-length	キー フィールドとして IPv6 ペイロード長を設定します。
Precedence	キー フィールドとして IPv6 precedence（ToS の一部）を設定します。
protocol	キー フィールドとして IPv6 プロトコルを設定します。
tos	キーフィールドとして IPv6 ToS を設定します。
traffic-class	キー フィールドとして IPv6 トラフィック クラスを設定します。

version	キー フィールドとして IPv6 ヘッダーから IPv6 バージョンを設定します。

コマンド デフォルト

IPv6 フィールドはキー フィールドとして設定されません。

コマンド モード

Flexible NetFlow フロー レコード コンフィギュレーション（config-flow-record）

コマンド履歴

リリース	変更内容
12.4(20)T	このコマンドが導入されました。
12.2(33)SRE	このコマンドが変更されました。 このコマンドのサポートが Cisco 7200 および Cisco 7300 ネットワーク処理エンジン（NPE）シリーズ ルータに実装されました。
12.2(50)SY	このコマンドが変更されました。 **flow-label**、**next-header**、**payload-length**、**traffic-class**、および **version** キーワードが削除されました。
15.2(2)T	このコマンドが変更されました。 Cisco Performance Monitor のサポートが追加されました。
Cisco IOS XE Release 3.5S	このコマンドが変更されました。 Cisco Performance Monitor のサポートが追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが変更されました。 **dscp**、**flow-label**、**next-header**、**payload-length**、および **precedence** キーワードが削除されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。 これらの製品は、このコマンドを発行するコンフィギュレーション モードを開始するために異なるコマンドを使用しますが、モード プロンプトは両方の製品で同じです。 Performance Monitor では、このコマンドを使用する前に、**flow record type performance-monitor** コマンドを入力します。

モード プロンプトが両方の製品で同じであるため、ここでは両方の製品のコマンド モードをフロー レコード コンフィギュレーション モードと呼びます。 ただし、Flexible NetFlow では、モードは Flexible NetFlow フロー レコード コンフィギュレーション モードとも呼ばれます。Performance Monitor では、モードは Performance Monitor フロー レコード コンフィギュレーション モードとも呼ばれます。

フロー レコードは、フロー モニタで使用する前に、少なくとも 1 つのキー フィールドを必要とします。 キー フィールドは、各フローがキー フィールドの値の一意のセットを持つことで、フローを区別します。 キー フィールドは、**match** コマンドを使用して定義されます。

（注） **match ipv6** コマンドのキーワードの一部は別のコマンドとして説明します。 別に記載されている **match ipv6** コマンドのすべてのキーワードは、**match ipv6** で始まります。 たとえば、フロー レコードのキー フィールドとして IPv6 ホップ制限を設定する方法の詳細については、**match ipv6 hop-limit** コマンドを参照してください。

例

次に、キー フィールドとして IPv6 DSCP フィールドを設定する例を示します。

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 dscp
```

次に、キー フィールドとして IPv6 DSCP フィールドを設定する例を示します。

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 dscp
```

関連コマンド

コマンド	説明
flow record	フロー レコードを作成し、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始します。
flow record type performance-monitor	フロー レコードを作成し、Performance Monitor フロー レコード コンフィギュレーション モードを開始します。

match ipv6 access-list

承認されたプレフィックスリストからの検査対象メッセージに含まれる送信者のIPv6アドレスを確認するには、RA ガード ポリシー コンフィギュレーション モードで **match ipv6 access-list** コマンドを使用します。

match ipv6 access-list *ipv6-access-list-name*

構文の説明

ipv6-access-list-name	照合される IPv6 アクセス リスト。

コマンド デフォルト

送信者の IPv6 アドレスは確認されません。

コマンド モード

RA ガード ポリシー コンフィギュレーション（config-ra-guard）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.2(4)S	このコマンドが Cisco IOS Release 15.2(4)S に統合されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

match ipv6 access-list コマンドは、設定された承認済みルータの送信元アクセス リストからの検査対象メッセージに含まれる送信者の IPv6 アドレスの検証をイネーブルにします。 **match ipv6 access-list** コマンドが設定されていない場合、この承認はバイパスされます。

アクセスリストは **ipv6 access-list** コマンドを使用して設定されます。 たとえば、リンクローカル アドレス FE80::A8BB:CCFF:FE01:F700 のルータだけを承認するには、次の IPv6 アクセス リストを定義します。

```
Router(config)# ipv6 access-list list1
Router(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any
```

（注） ここでは、アクセス リストを複数の明示的なルータ ソースを定義する便利な方法として使用していますが、ポートベースのアクセス リスト（PACL）ではありません。**match ipv6 access-list** コマンドは、ルータ メッセージの IPv6 送信元アドレスを検証するため、アクセス リストで宛先を指定することには意味がありません。アクセス コントロール リスト（ACL）のエントリの宛先は常に「Any」にする必要があります。宛先がアクセス リストで指定されている場合、照合が失敗します。

例

次に、ルータ アドバタイズメント（RA）ガード ポリシー名を raguard1 として定義し、ルータを RA ガード ポリシー コンフィギュレーション モードにして、list1 という名前のアクセス リストの IPv6 アドレスと照合する例を示します。

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# match ipv6 access-list list1
```

関連コマンド

コマンド	説明
ipv6 nd raguard policy	RA ガード ポリシー名を定義し、RA ガード ポリシー コンフィギュレーション モードを開始します。
ipv6 access-list	IPv6 アクセス リストを定義し、ルータを IPv6 アクセス リスト コンフィギュレーション モードにします。

match ipv6 address

プレフィックス リストで許可されたプレフィックスを持つ IPv6 ルートを配布する、または IPv6 のポリシーベース ルーティング（PBR）用にパケットを照合するために使用する IPv6 アクセス リストを指定するには、ルートマップ コンフィギュレーション モードで **match ipv6 address** コマンドを使用します。 **match ipv6 address** エントリを削除するには、このコマンドの **no** 形式を使用します。

match ipv6 address {**prefix-list** *prefix-list-name*| *access-list-name*}

no match ipv6 address

構文の説明

prefix-list *prefix-list-name*	IPv6 プレフィックス リストの名前を指定します。
access-list-name	IPv6 アクセス リスト名。 名前にはスペースまたは引用符を含めることはできません。また、数字で始めることはできません。

コマンド デフォルト

宛先ネットワーク番号またはアクセス リストに基づいて配布されるルートはありません。

コマンド モード

ルートマップ コンフィギュレーション（config-route-map）

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.3(7)T	このコマンドが変更されました。 引数 *access-list-name* が追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。

リリース	変更内容
12.2(33)SXI4	このコマンドが変更されました。 **prefix-list** *prefix-list-name* キーワード/引数ペアの引数は、Cisco IOS Release 12.2(33)SXI4 ではサポートされません。
Cisco IOS XE Release 3.2S	このコマンドが Cisco IOS XE Release 3.2SG に統合されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

route-map コマンドと **match** および **set** コマンドを使用して、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。 **route-map** コマンドごとに、それに関連した **match** および **set** コマンドのリストがあります。 **match** コマンドは、一致基準、つまり現在の **route-map** コマンドについて再配布を許可する条件を指定します。 **set** コマンドは、**match** コマンドによって強制される基準が満たされた場合に実行される特定の再配布アクションである設定アクションを指定します。

match ipv6 address コマンドは、アクセス リストまたはプレフィックス リストを指定するために使用できます。 PBR を使用する場合は、*access-list-name* 引数を使用する必要があります。**prefix-list** *prefix-list-name* キーワード/引数ペアの引数は機能しません。

例

次の例では、marketing という名前のプレフィックス リストで指定されたアドレスを持つ IPv6 ルートが一致します。

```
Device(config)# route-map name
Device(config-route-map)# match ipv6 address prefix-list marketing
```

次の例では、marketing という名前のアクセス リストで指定されたアドレスを持つ IPv6 ルートが一致します。

```
Device(config)# route-map
Device(config-route-map)# match ipv6 address marketing
```

関連コマンド

コマンド	説明
match as-path	BGP 自律システム パス アクセス リストを照合します。
match community	BGP コミュニティを照合します。
match ipv6 address	IPv6 の PBR のパケットと照合するために使用する IPv6 アクセス リストを指定します。

コマンド	説明
match ipv6 next-hop	プレフィックス リストによって許可されているネクスト ホップ プレフィックスを持つ IPv6 ルートを配布します。
match ipv6 route-source	プレフィックス リストに指定されているアドレスのルータによってアドバタイズされた IPv6 ルートを配布します。
match length	パケットのレベル 3 長に基づいてポリシー ルーティングを実行します。
match metric	指定したメトリックを持つルートを再配布します。
match route-type	指定されたタイプのルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
set as-path	BGP ルートの自律システム パスを変更します。
set community	BGP コミュニティ属性を設定します。
set default interface	ポリシー ルーティング用のルート マップの match 句を通過し、宛先への明示的ルートがないパケットを出力するデフォルト インターフェイスを指定します。
set interface	ポリシー ルーティング用のルート マップの match 句を通過したパケットを出力するデフォルト インターフェイスを指定します。
set ipv6 default next-hop	一致パケットが転送されるデフォルトの IPv6 ネクスト ホップを指定します。
set ipv6 next-hop（PBR）	ポリシー ルーティング用のルート マップの match 句を通過した IPv6 パケットの送出先を示します。
set ipv6 precedence	IPv6 パケット ヘッダーのプリファレンス値を設定します。
set level	ルートのインポート先を示します。

コマンド	説明
set local preference	自律システムパスのプリファレンス値を指定します。
set metric	ルーティングプロトコルのメトリック値を設定します。
set metric-type	宛先ルーティング プロトコルのメトリック タイプを設定します。
set tag	宛先ルーティングプロトコルのタグ値を設定します。
set weight	ルーティング プロトコルの BGP 重みを指定します。

match ipv6 destination

フロー レコードのキー フィールドとして IPv6 宛先アドレスを設定するには、Flexible NetFlow フロー レコード コンフィギュレーション モードで **match ipv6 destination** コマンドを使用します。フロー レコードのキー フィールドとしての IPv6 宛先アドレスをディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv6 destination {**address**| {**mask**| **prefix**} [**minimum-mask** *mask*]}

no match ipv6 destination {**address**| {**mask**| **prefix**} [**minimum-mask** *mask*]}

Cisco Catalyst 6500 Switches in Cisco IOS Release 12.2(50)SY

match ipv6 destination address

no match ipv6 destination address

Cisco IOS XE Release 3.2SE

match ipv6 destination address

no match ipv6 destination address

構文の説明

address	キー フィールドとして IPv6 宛先アドレスを設定します。
mask	キー フィールドとして IPv6 宛先アドレスのマスクを設定します。
prefix	キー フィールドとして IPv6 宛先アドレスのプレフィックスを設定します。
minimum-mask *mask*	（任意）最小マスクのサイズをビット単位で指定します。 有効な範囲は、1 ～ 128 です。

コマンド デフォルト

IPv6 宛先アドレスはキー フィールドとして設定されません。

コマンド モード

Flexible NetFlow フロー レコード コンフィギュレーション（config-flow-record）

コマンド履歴

リリース	変更内容
12.4(20)T	このコマンドが導入されました。
12.2(33)SRE	このコマンドが変更されました。 このコマンドのサポートが Cisco 7200 および Cisco 7300 ネットワーク処理エンジン（NPE）シリーズ ルータに実装されました。
12.2(50)SY	このコマンドが変更されました。 **mask**、**prefix**、および **minimum-mask** キーワードが削除されました。
15.2(2)T	このコマンドが変更されました。 Cisco Performance Monitor のサポートが追加されました。
Cisco IOS XE Release 3.5S	このコマンドが変更されました。 Cisco Performance Monitor のサポートが追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが変更されました。 **mask**、**prefix**、および **minimum-mask** キーワードが削除されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。 これらの製品は、このコマンドを発行するコンフィギュレーション モードを開始するために異なるコマンドを使用しますが、モード プロンプトは両方の製品で同じです。 Performance Monitor では、このコマンドを使用する前に、**flow record type performance-monitor** コマンドを入力します。

モード プロンプトが両方の製品で同じであるため、ここでは両方の製品のコマンド モードをフロー レコード コンフィギュレーション モードと呼びます。 ただし、Flexible NetFlow では、モードは Flexible NetFlow フロー レコード コンフィギュレーション モードとも呼ばれます。Performance Monitor では、モードは Performance Monitor フロー レコード コンフィギュレーション モードとも呼ばれます。

フロー レコードは、フロー モニタで使用する前に、少なくとも 1 つのキー フィールドを必要とします。 キー フィールドは、各フローがキー フィールドの値の一意のセットを持つことで、フローを区別します。 キー フィールドは、**match** コマンドを使用して定義されます。

例

次に、キー フィールドとして 16 ビット IPv6 宛先アドレス プレフィックスを設定する例を示します。

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 destination prefix minimum-mask 16
```

次に、キー フィールドとして 16 ビット IPv6 宛先アドレス マスクを指定する例を示します。

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 destination mask minimum-mask 16
```

次に、キー フィールドとして 16 ビット IPv6 宛先アドレス マスクを設定する例を示します。

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 destination mask minimum-mask 16
```

関連コマンド

コマンド	説明
flow record	フロー レコードを作成し、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始します。
flow record type performance-monitor	フロー レコードを作成し、Performance Monitor フロー レコード コンフィギュレーション モードを開始します。

match ipv6 hop-limit

フロー レコードのキー フィールドとしてIPv6ホップ制限を設定するには、Flexible NetFlowフロー レコード コンフィギュレーション モードで **match ipv6 hop-limit** コマンドを使用します。 フロー レコードのキーフィールドとしてIPv6パケットのセクションの使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv6 hop-limit

no match ipv6 hop-limit

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ユーザ定義のフロー レコードのキー フィールドとして IPv6 ホップ制限を使用することはデフォルトでイネーブルになっていません。

コマンド モード

Flexible NetFlow フロー レコード コンフィギュレーション（config-flow-record）

コマンド履歴

リリース	変更内容
12.4(20)T	このコマンドが導入されました。
12.2(33)SRE	このコマンドが変更されました。 このコマンドのサポートがCisco 7200 およびCisco 7300 ネットワーク処理エンジン（NPE）シリーズ ルータに実装されました。
15.2(2)T	このコマンドが変更されました。 Cisco Performance Monitor のサポートが追加されました。
Cisco IOS XE Release 3.5S	このコマンドが変更されました。 Cisco Performance Monitor のサポートが追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。 これらの製品は、このコマンドを発行するコンフィギュレーション モードを開始するために異なるコマンドを使用しますが、モード プロンプトは両方の製品で同じです。 Performance Monitor では、このコマンドを使用する前に、**flow record type performance-monitor** コマンドを入力します。

モード プロンプトが両方の製品で同じであるため、ここでは両方の製品のコマンド モードをフロー レコード コンフィギュレーション モードと呼びます。 ただし、Flexible NetFlow では、モードはFlexible NetFlowフロー レコードコンフィギュレーションモードとも呼ばれます。Performance Monitor では、モードは Performance Monitor フロー レコード コンフィギュレーション モードとも呼ばれます。

フロー レコードは、フロー モニタで使用する前に、少なくとも 1 つのキー フィールドを必要とします。 キー フィールドは、各フローがキー フィールドの値の一意のセットを持つことで、フローを区別します。 キー フィールドは、**match** コマンドを使用して定義されます。

例

次に、キー フィールドとしてパケットのホップ制限をフローで設定する例を示します。

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 hop-limit
```

次に、キー フィールドとしてパケットのホップ制限をフローで設定する例を示します。

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 hop-limit
```

関連コマンド

コマンド	説明
flow record	フロー レコードを作成し、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始します。
flow record type performance-monitor	フロー レコードを作成し、Performance Monitor フロー レコード コンフィギュレーション モードを開始します。

match ra prefix-list

承認されたプレフィックス リストからの検査対象メッセージに含まれるアドバタイズされたプレフィックスを確認するには、RA ガード ポリシー コンフィギュレーション モードで **match ra prefix-list** コマンドを使用します。

match ra prefix-list *ipv6-prefix-list-name*

構文の説明

ipv6-prefix-list-name	照合される IPv6 プレフィックスのリスト。

コマンド デフォルト

アドバタイズされたプレフィックスは確認されません。

コマンド モード

RA ガード ポリシー コンフィギュレーション（config-ra-guard）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.2(4)S	このコマンドが Cisco IOS Release 15.2(4)S に統合されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

match ra prefix-list コマンドは、設定された承認済みルータのプレフィックス リストからの検査対象メッセージに含まれるアドバタイズされたプレフィックスの検証をイネーブルにします。 IPv6 プレフィックス リストを設定するには **ipv6 prefix-list** コマンドを使用します。 たとえば、プレフィックス 2001:101::/64 を承認し、プレフィックス 2001:100::/64 を拒否するには、次の IPv6 プレフィックス リストを定義します。

```
Router(config)# ipv6 prefix-list listname1 deny 2001:0DB8:101:/64
Router(config)# ipv6 prefix-list listname1 permit 2001:0DB8:100::/64
```

例

次に、ルータ アドバタイズメント（RA）ガード ポリシー名を raguard1 として定義し、ルータを RA ガード ポリシー コンフィギュレーション モードにして、listname1 のアドバタイズされたプレフィックスを検証する例を示します。

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# match ra prefix-list listname1
```

関連コマンド

コマンド	説明
ipv6 nd raguard policy	RA ガード ポリシー名を定義し、RA ガード ポリシー コンフィギュレーション モードを開始します。
ipv6 prefix-list	IPv6 プレフィックス リストのエントリを作成します。

max-through

スロットル期間ごとの VLAN 単位のマルチキャスト ルータ アドバタイズメント（RA）を制限するには、IPv6 RA スロットル ポリシー コンフィギュレーション モードで **max-through** を使用します。 コマンドをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

max-through {*mt-value*| **inherit**| **no-limit**}

構文の説明

mt-value	スロットリングが発生するまでに VLAN で許可されるマルチキャスト RA 数。 指定できる範囲は 0 ～ 256 です。
inherit	ターゲット ポリシー間の設定をマージします。
no-limit	マルチキャスト RA は VLAN で制限されません。

コマンド デフォルト

10 分あたり VLAN あたり 10 RA

コマンド モード

IPv6 RA スロットル ポリシー コンフィギュレーション（config-nd-ra-throttle）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2XE	このコマンドが導入されました。

使用上のガイドライン

max-through コマンドで、スロットル期間ごとに VLAN へパススルーされるマルチキャスト RA の量を制限します。 このコマンドは、VLAN 上でのみ設定できます。

例

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# max-through 25
```

medium-type

デバイスが有線か無線かを示すには、IPv6 RA スロットル ポリシー コンフィギュレーション モードで **media-type** コマンドを使用します。 コマンドをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

medium-type {**access-point**| **wired**}

構文の説明

access-point	接続デバイスは無線アクセスポイントで、スロットリングされます。
wired	接続デバイスは有線で、スロットリングされません。

コマンド デフォルト

有線

コマンド モード

IPv6 RA スロットル ポリシー コンフィギュレーション（config-nd-ra-throttle）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release XE3.2S	このコマンドが導入されました。

使用上のガイドライン

medium-type コマンドは、ポートのアクセスのタイプだけを示します。 VLAN は、**media-type** コマンドで指定された値を無視します。

例

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# medium-type wired
```

mode dad-proxy

IPv6 ネイバー探索（ND）抑制のために重複アドレス検出（DAD）プロキシ モードをイネーブルにするには、ND 抑制ポリシー コンフィギュレーション モードで **mode dad-proxy** コマンドを使用します。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

mode dad-proxy

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

マルチキャスト ネイバー送信要求（NS）のすべてのメッセージが抑制されます。

コマンド モード

ND 抑制ポリシー コンフィギュレーション モード（config-nd-suppress）

コマンド履歴

リリース	変更内容
15.1(2)SG	このコマンドが導入されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

IPv6 DAD プロキシ機能は、アドレスがすでに使用されている場合に、アドレスの所有者に代わって応答します。 IPv6 ND 抑制の使用時に IPv6 DAD プロキシをイネーブルにするには、**mode dad-proxy** コマンドを使用します。 デバイスが IPv6 マルチキャスト抑制をサポートしない場合は、グローバル コンフィギュレーション モードで **ipv6 nd dad-proxy** コマンドを入力して、IPv6 DAD プロキシをイネーブルにできます。

例

```
Device(config)# ipv6 nd suppress policy policy1
Device(config-nd-suppress)# mode dad-proxy
```

関連コマンド

コマンド	説明
ipv6 nd dad-proxy	デバイスの IPv6 ND DAD プロキシ機能をイネーブルにします。

コマンド	説明
ipv6 nd suppress policy	IPv6 ND マルチキャスト抑制をイネーブルにして、ND 抑制ポリシー コンフィギュレーション モードを開始します。

network（IPv6）

ネクスト ホップのネットワーク ソースを PE VPN で使用されるように設定するには、ルータ コンフィギュレーション モードで network コマンドを使用します。 ソースをディセーブルにするには、このコマンドの **no** 形式を使用します。

network *ipv6-address/prefix-length*

no network *ipv6-address/prefix-length*

構文の説明

ipv6-address	使用する IPv6 アドレス。
/ *prefix-length*	IPv6 プレフィックスの長さ。 プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す10進値です。10 進数値の前にスラッシュ記号が必要です。

コマンド デフォルト

ネクスト ホップのネットワーク ソースは設定されていません。

コマンド モード

アドレス ファミリ コンフィギュレーション ルータ コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが導入されました。
12.2(33)SB	このコマンドが、Cisco IOS Release 12.2(33)SB に統合されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI に統合されました。
Cisco IOS XE Release 3.1S	このコマンドが Cisco IOS XE Release 3.1S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

このコマンドの *ipv6-address* 引数は、IPv6 ネットワーク番号を設定します。

例

次に、ルータをアドレス ファミリ コンフィギュレーション モードにし、ネットワーク ソースをネクスト ホップとして使用するように設定します。

```
Router(config)# router bgp 100
Router(config-router)# network 2001:DB8:100::1/128
```

関連コマンド

コマンド	説明
address-family ipv6	標準 IPv6 アドレス プレフィックスを使用する BGP などのルーティング セッションを設定するために、アドレス ファミリ コンフィギュレーション モードを開始します。
address-family vpnv6	標準 VPNv6 アドレス プレフィックスを使用するルーティング セッションを設定するために、ルータをアドレス ファミリ コンフィギュレーション モードにします。

other-config-flag

アドバタイズされた「その他」の設定パラメータを確認するには、RA ガード ポリシー コンフィギュレーション モードで **other-config-flag** コマンドを使用します。

other-config-flag {**on**| **off**}

構文の説明

on	検証はイネーブルです。
off	検証はディセーブルです。

コマンド デフォルト

検証はイネーブルになりません。

コマンド モード

RA ガード ポリシー コンフィギュレーション（config-ra-guard）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.2(4)S	このコマンドが Cisco IOS Release 15.2(4)S に統合されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

other-config-flag コマンドによって、アドバタイズされた「その他」の設定パラメータ（「O」フラグ）を検証できます。 このフラグは、信頼できない可能性がある Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバを通じてホストにその他の設定情報を取得させるために、攻撃者によって設定されることがあります。

例

次に、ルータ アドバタイズメント（RA）ガード ポリシー名を raguard1 として定義し、ルータを RA ガード ポリシー コンフィギュレーション モードにして、O フラグの検証をイネーブルにする例を示します。

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# other-config-flag on
```

関連コマンド

コマンド	説明
ipv6 nd raguard policy	RA ガード ポリシー名を定義し、RA ガード ポリシー コンフィギュレーション モードを開始します。

passive-interface（IPv6）

インターフェイス上のルーティングアップデートの送信をディセーブルにするには、ルータ コンフィギュレーション モードで **passive-interface** コマンドを使用します。 ルーティング アップデートの送信を再度イネーブルにするには、このコマンドの **no** 形式を使用します。

passive-interface [**default**| *interface-type interface-number*]

no passive-interface [**default**| *interface-type interface-number*]

構文の説明

default	（任意）すべてのインターフェイスがパッシブとなります。
interface-type interface-number	（任意）インターフェイス タイプおよび番号 詳細については、疑問符（**?**）オンライン ヘルプ機能を使用します。

コマンド デフォルト

インターフェイスはパッシブではありません。 ルーティング アップデートは、ルーティング プロトコルがイネーブルであるすべてのインターフェイスに送信されます。

コマンド モード

ルータ コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(15)T	このコマンドが導入されました。
12.4(6)T	Enhanced Interior Gateway Routing Protocol（EIGRP）IPv6 のサポートが追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRB	このコマンドが、Cisco IOS Release 12.2(33)SRB に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

インターフェイス上でルーティング アップデートの送信をディセーブルにした場合でも、特定のアドレス プレフィックスは引き続き他のインターフェイスにアドバタイズされ、このインターフェイス上の他のルータからのアップデートは引き続き受信および処理されます。

default キーワードを指定すると、すべてのインターフェイスがデフォルトでパッシブに設定されます。 この場合、隣接情報を必要とする個別のインターフェイスを設定するには、**no passive-interface** コマンドを使用します。 **default** キーワードは、インターネット サービス プロバイダー（ISP）や大規模な企業ネットワークなど、多数のディストリビューション ルータに 200 以上ものインターフェイスが搭載されるような環境で役立ちます。

OSPF for IPv6 ルーティング情報は、指定されたルータ インターフェイスから送受信されません。指定したインターフェイス アドレスは、OSPF for IPv6 ドメイン内のスタブ ネットワークとして表示されます。

Intermediate System-to-Intermediate System（IS-IS）プロトコルの場合、このコマンドでは IS-IS に対し、指定したインターフェイスでは実際に IS-IS を実行せずに、このインターフェイスの IP アドレスをアドバタイズするように指示します。 IS-IS に対してこのコマンドの **no** 形式を使用すると、指定したアドレスの IP アドレスのアドバタイズがディセーブルになります。

例

次の例では、すべてのインターフェイスをパッシブに設定してから、インターフェイス ethernet0 をアクティブにする方法を示します。

```
Router(config-router)# passive-interface default
Router(config-router)# no passive-interface ethernet0/0
```

passive-interface（OSPFv3）

IPv4 Open Shortest Path First バージョン 3（OSPFv3）プロセスを使用するときに、インターフェイスのルーティング アップデートの送信を抑制するには、ルータ コンフィギュレーション モードで **passive-interface** コマンドを使用します。 ルーティング アップデートの送信を再度イネーブルにするには、このコマンドの **no** 形式を使用します。

passive-interface [**default**| *interface-type interface-number*]

no passive-interface [**default**| *interface-type interface-number*]

構文の説明

default	（任意）すべてのインターフェイスがパッシブとなります。
interface-type interface-number	（任意）インターフェイス タイプおよび番号 詳細については、疑問符（**?**）オンライン ヘルプ機能を使用します。

コマンド デフォルト

インターフェイスはパッシブではありません。 ルーティング アップデートは、ルーティング プロトコルがイネーブルであるすべてのインターフェイスに送信されます。

コマンド モード

OSPFv3 ルータ コンフィギュレーション モード（config-router）

コマンド履歴

リリース	変更内容
15.1(3)S	このコマンドが導入されました。
Cisco IOS XE Release 3.4S	このコマンドが Cisco IOS XE Release 3.4S に統合されました。
15.2(1)T	このコマンドが Cisco IOS Release 15.2(1)T に統合されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

インターフェイス上でルーティングアップデートの送信を抑制した場合でも、特定のアドレスプレフィックスは引き続き他のインターフェイスにアドバタイズされ、このインターフェイス上の他のルータからのアップデートは引き続き受信および処理されます。

default キーワードを指定すると、すべてのインターフェイスがデフォルトでパッシブに設定されます。 この場合、隣接情報を必要とする個別のインターフェイスを設定するには、**no passive-interface** コマンドを使用します。 **default** キーワードは、インターネット サービス プロバイダー（ISP）や大規模な企業ネットワークなど、多数のディストリビューション ルータに 200 以上ものインターフェイスが搭載されるような環境で役立ちます。

例

次の例では、すべてのインターフェイスをパッシブに設定してから、イーサネット インターフェイス 0/0 をアクティブにする方法を示します。

```
Router(config-router)# passive-interface default
Router(config-router)# no passive-interface ethernet0/0
```

関連コマンド

コマンド	説明
default（OSPFv3）	OSPFv3 パラメータをデフォルト値に戻します。
router ospfv3	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。

permit（IPv6）

IPv6 アクセス リストの許可条件を設定するには、IPv6 アクセス リスト コンフィギュレーション モードで **permit** コマンドを使用します。 許可条件を削除するには、このコマンドの **no** 形式を使用します。

permit *protocol* {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] [**reflect** *name* [**timeout** *value*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

no permit *protocol* {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] [**reflect** *name* [**timeout** *value*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Internet Control Message Protocol

permit icmp {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*]| *icmp-message*] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Transmission Control Protocol

permit tcp {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] **[ack]** [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] **[established] [fin]** [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] [**neq** {*port*| *protocol*}] **[psh]** [**range** {*port*| *protocol*}] [**reflect** *name* [**timeout** *value*]] **[routing]** [**routing-type** *routing-number*] **[rst]** [**sequence** *value*] **[syn]** [**time-range** *name*] **[urg]**

User Datagram Protocol

permit udp {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] [**neq** {*port*| *protocol*}] [**range** {*port*| *protocol*}] [**reflect** *name* [**timeout** *value*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

構文の説明

protocol	インターネットプロトコルの名前または番号。これは、キーワード **ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**sctp**、**tcp**、**udp**、または **hbh** にするか、IPv6 プロトコル番号を表す 0 ～ 255 の整数にすることができます。
source-ipv6-prefix/prefix-length	許可条件を設定する送信元 IPv6 ネットワークまたはネットワークのクラス。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
any	IPv6 プレフィックス ::/0 の省略形。
host *source-ipv6-address*	許可条件の設定先である送信元 IPv6 ホスト アドレス。 この *source-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
auth	任意のプロトコルと組み合わせて、認証ヘッダーのプレゼンスとトラフィックを照合できます。

operator [*port-number*]	（任意）指定のプロトコルの送信元または宛先ポートを比較するオペランドを指定します。オペランドには、**lt**（less than：より小さい）、**gt**（greater than：より大きい）、**eq**（equal：等しい）、**neq**（not equal：等しくない）、および **range**（inclusive range：包含範囲）があります。 *source-ipv6-prefix*/*prefix-length* 引数の後ろに演算子が置かれた場合、送信元ポートと一致する必要があります。 *destination-ipv6-prefix*/*prefix-length* 引数の後ろに演算子が置かれた場合、宛先ポートと一致する必要があります。 **range** 演算子には 2 つのポート番号が必要です。他のすべての演算子は 1 つのポート番号が必要です。 任意の *port-number* 引数は 10 進数、または TCP あるいは UDP ポートの名前です。 ポート番号の範囲は 0 ～ 65535 です。 TCP ポート名は TCP をフィルタリングする場合に限り使用できます。 UDP ポート名は UDP をフィルタリングする場合に限り使用できます。
destination-ipv6-prefix/*prefix-length*	許可条件を設定する宛先 IPv6 ネットワーク、またはネットワークのクラス。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
host *destination-ipv6-address*	許可条件の設定先である宛先 IPv6 ホスト アドレス。 この *destination-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
dest-option-type	（任意）各 IPv6 パケット ヘッダー内の宛先拡張ヘッダーと IPv6 パケットを照合します。
doh-number	（任意）IPv6 宛先オプション拡張ヘッダーを表す 0 から 255 の範囲の整数。

doh-type	（任意）宛先オプション ヘッダー タイプ。 可能な宛先オプション ヘッダー タイプおよび対応する *doh-number* 値は、home-address と 201 です。
dscp *value*	（任意）各 IPv6 パケット ヘッダーのトラフィック クラス フィールドのトラフィック クラス値と DiffServ コード ポイント値を照合します。 指定できる範囲は 0 ～ 63 です。
flow-label *value*	（任意）各 IPv6 パケット ヘッダーのフロー ラベル フィールドのフロー ラベルの値とフロー ラベルの値を照合します。 指定できる範囲は 0 ～ 1048575 です。
fragments	（任意）フラグメント拡張ヘッダーに 0 以外のフラグメント オフセットが含まれる場合、非初期フラグメント パケットを照合します。 **fragments** キーワードは、*operator* [*port-number*] 引数が指定されていない場合に限り指定できるオプションです。 このキーワードが使用されている場合、最初のフラグメントにレイヤ 4 情報が含まれていない場合にも照合を行います。
hbh	（任意）各 IPv6 パケット ヘッダー内のホップバイホップ拡張ヘッダーと IPv6 パケットを照合します。
log	（任意）コンソールに送信されるエントリに一致するパケットに関するロギング メッセージ情報が出力されます。 コンソールにロギングするメッセージのレベルは、**logging console** コマンドで制御します。 このメッセージに含まれるものには、アクセス リスト名とシーケンス番号、パケットが許可されたか、プロトコルが TCP、UDP、ICMP、または番号であったか、さらに、該当する場合は、送信元と宛先アドレス、および送信元と宛先ポート番号があります。 メッセージは、一致した最初のパケットに対して生成され、その後、5 分間隔で許可されたパケット数を含めて生成されます。

log-input	（任意）ロギング メッセージに入力インターフェイスも含まれることを除き、**log** キーワードと同じ機能を提供します。
mobility	（mobility）各 IPv6 パケット ヘッダー内のモビリティ拡張ヘッダーと IPv6 パケットを照合します。
mobility-type	（任意）各 IPv6 パケット ヘッダー内のモビリティ タイプ拡張ヘッダーと IPv6 パケットを照合します。 このキーワードと共に、*mh-number* または *mh-type* 引数を使用する必要があります。
mh-number	（任意）IPv6 モビリティ ヘッダー タイプを表す 0 から 255 の範囲の整数。
mh-type	（任意）モビリティ ヘッダー タイプ。 次のようなモビリティ ヘッダー タイプと対応する *mh-number* 値が可能です。 • 0：bind-refresh • 1：hoti • 2：coti • 3：hot • 4：cot • 5：bind-update • 6：bind-acknowledgment • 7：bind-error
reflect *name*	（任意）再帰 IPv6 アクセス リストを指定します。 再帰 IPv6 アクセス リストは、IPv6 パケットが **reflect** キーワードを含む permit ステートメントに一致すると動的に作成されます。 再帰 IPv6 アクセス リストは、permit ステートメントに一致する IPv6 パケットがない場合、permit ステートメントをミラーリングし、自動的にタイムアウトします。 再帰 IPv6 アクセス リストは、IPv6 パケットの TCP、UDP、SCTP、および ICMP に適用できます。

timeout *value*	（任意）再帰 IPv6 アクセス リストがタイムアウトになる前のアイドル時間の間隔（秒単位）。 指定できる範囲は 1 ～ 4294967295 です。 デフォルト値は 180 秒です。
routing	（任意）ソースルート パケットを、各 IPv6 パケット ヘッダー内の拡張ヘッダーに一致させます。
routing-type	（任意）各 IPv6 パケット ヘッダー内のルーティング タイプ拡張ヘッダーと IPv6 パケットを照合します。 このキーワードと共に、*routing-number* 引数を使用する必要があります。
routing-number	IPv6 ルーティング ヘッダー タイプを表す 0 から 255 の範囲の整数。 次のようなルーティング ヘッダー タイプと対応する *routing-number* 値が可能です。 • 0：標準 IPv6 ルーティング ヘッダー • 2：モバイル IPv6 ルーティング ヘッダー
sequence *value*	（任意）アクセス リスト ステートメントのシーケンス番号を指定します。 指定できる範囲は 1 ～ 4294967295 です。
time-range *name*	（任意）許可ステートメントに適用する時間範囲を指定します。 時間範囲の名前と制限事項は、**time-range** コマンドと、**absolute** または **periodic** コマンドによってそれぞれ指定します。
icmp-type	（任意）ICMP パケットのフィルタリングに ICMP メッセージ タイプを指定します。 ICMP パケットは、ICMP メッセージ タイプでフィルタリングできます。 ICMP メッセージ タイプは、0 ～ 255 の数字で、次のような事前定義された文字列とそれに対応する数値が含まれています。 • 144：dhaad-request • 145：dhaad-reply • 146：mpd-solicitation • 147：mpd-advertisement

icmp-code	（任意）ICMP パケットのフィルタリングに ICMP メッセージ コードを指定します。 ICMP メッセージタイプによってフィルタリングされる ICMP パケットは、ICMP メッセージ コードによってもフィルタリングできます。 メッセージ コードの番号は 0 ～ 255 です。
icmp-message	（任意）ICMP パケットのフィルタリングに ICMP メッセージ名を指定します。 ICMP パケットは、ICMP メッセージ名、または ICMP メッセージタイプおよびコードによってフィルタリングできます。 使用可能な名前については、「使用上のガイドライン」を参照してください。
ack	（任意）TCP プロトコルの場合に限り ACK ビットを設定します。
established	（任意）TCP プロトコルの場合にだけ、確立された接続を表示します。 TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。 接続するための初期 TCP データグラムの場合は照合しません。
fin	（任意）TCP プロトコルの場合に限り、FIN ビットを設定します。送信元からのデータはこれ以上ありません。
neq {*port* | *protocol*}	（任意）指定のポート番号上にないパケットだけを照合します。
psh	（任意）TCP プロトコルの場合に限り PSH ビットを設定します。
{**range** *port* | *protocol*}	（任意）ポート番号範囲のパケットだけを照合します。
rst	（任意）TCP プロトコルの場合に限り RST ビットを設定します。
syn	（任意）TCP プロトコルの場合に限り SYN ビットを設定します。
urg	（任意）TCP プロトコルの場合に限り URG ビットを設定します。

コマンド デフォルト

IPv6 アクセス リストは定義されていません。

コマンド モード

IPv6 アクセス リスト コンフィギュレーション (config-ipv6-acl)#

コマンド履歴

リリース	変更内容
12.0(23)S	このコマンドが導入されました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.4(2)T	*icmp-type* 引数が拡張されました。 **dest-option-type**、**mobility**、**mobility-type** および **routing-type** キーワードが追加されました。*doh-number*、*doh-type*、*mh-number*、*mh-type* および *routing-number* 引数が追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ ルータで追加されました。
12.4(20)T	**auth** キーワードが追加されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
15.2(3)T	このコマンドが変更されました。 **hbh** キーワードのサポートが追加されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

permit（IPv6）コマンドは、IPv6に固有のものを除き、**permit**（IP）コマンドと類似しています。

ipv6 access-list コマンドに続いて、**permit**（IPv6）コマンドを使用すると、パケットがアクセス リストを通過する条件を定義すること、または再帰アクセスリストとしてアクセスリストを定義することができます。

protocol 引数に IPv6 を指定すると、パケットの IPv6 ヘッダーに対して照合を行います。

デフォルトでは、アクセス リストの最初のステートメントは 10 で、その次のステートメントからは 10 ずつ増加します。

permit、**deny**、**remark**、または **evaluate** ステートメントを、リスト全体を再入力せずに既存のアクセスリストに追加できます。新しいステートメントをリストの最後尾以外に追加するには、所属先を示すために 2 つの既存のエントリ番号の間にある適切なエントリ番号を持つ新しいステートメントを作成します。

Cisco IOS Release 12.2(2)T 以降のリリース、12.0(21)ST、および 12.0(22)S では、IPv6 アクセス コントロール リスト（ACL）の定義、および拒否条件と許可条件の設定は、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドと **deny** および **permit** キーワードを使用して行います。 Cisco IOS Release 12.0(23)S 以降のリリースでは、IPv6 ACL は、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用することにより定義され、許可条件と拒否条件は、IPv6 アクセスリスト コンフィギュレーション モードで **deny** コマンドおよび **permit** コマンドを使用して設定されます。 IPv6 ACL の定義の詳細については、**ipv6 access-list** コマンドを参照してください。

（注） Cisco IOS Release 12.0(23)S 以降のリリースでは、IPv6 ACL に最後の一致条件として暗黙の **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および**deny ipv6 any any** ステートメントがあります。（前の 2 つの一致条件により ICMPv6 ネイバー探索が可能になります）。IPv6 ACL には、暗黙の **deny ipv6 any any** ステートメントを有効にするために少なくとも 1 つのエントリが含まれる必要があります。IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを利用するため、デフォルトで、インターフェイス上での IPv6 ネイバー探索パケットの送受信が IPv6 ACL によって暗黙的に許可されます。 IPv4 の場合、IPv6 ネイバー探索プロセスに相当するアドレス解決プロトコル（ARP）では、個別のデータ リンク層プロトコルを利用するため、デフォルトで、インターフェイス上での ARP パケットの送受信が IPv4 ACL によって暗黙的に許可されます。

source-ipv6-prefix/*prefix-length* と *destination-ipv6-prefix*/*prefix-length* の両方の引数をトラフィックのフィルタリングに使用します（送信元プレフィックスはトラフィックの送信元に基づいて、宛先プレフィックスはトラフィックの宛先に基づいてトラフィックをフィルタリングします）。

（注） アクセス リストでなく、IPv6 プレフィックス リストは、ルーティング プロトコル プレフィックスのフィルタリングに使用する必要があります。

fragments キーワードは、*operator* [*port-number*] 引数が指定されていない場合に限り指定できるオプションです。

次に、ICMP メッセージの名前のリストを示します。

- beyond-scope

- destination-unreachable
- echo-reply
- echo-request
- header
- hop-limit
- mld-query
- mld-reduction
- mld-report
- nd-na
- nd-ns
- next-header
- no-admin
- no-route
- packet-too-big
- parameter-option
- parameter-problem
- port-unreachable
- reassembly-timeout
- renum-command
- renum-result
- renum-seq-number
- router-advertisement
- router-renumbering
- router-solicitation
- time-exceeded
- unreachable

再帰アクセス リストの定義

セッション フィルタリングの形式でIPv6 再帰リストを定義するには、**permit**（IPv6）コマンドで **reflect** キーワードを使用します。 **reflect** キーワードは、IPv6 再帰アクセス リストを作成し、再帰アクセス リストのエントリの作成をトリガーします。 **reflect** キーワードは、IPv6 アクセス リストのエントリ（条件ステートメント）である必要があります。

（注） IPv6 再帰アクセス リストを機能させるには、**evaluate** コマンドを使用して再帰アクセス リストをネストする必要があります。

外部インターフェイスの IPv6 再帰アクセス リストを設定する場合、IPv6 アクセス リストはアウトバウンド トラフィックに適用されるものにする必要があります。

内部インターフェイスの IPv6 再帰アクセス リストを設定する場合、IPv6 アクセス リストはインバウンド トラフィックに適用されるものにする必要があります。

ネットワーク内から発信される IPv6 セッションは、ネットワークから出て行くパケットで開始されます。 このようなパケットが IPv6 アクセス リストのステートメントで評価されるとき、パケットは、IPv6 再帰許可エントリでも評価されます。

すべての IPv6 アクセス リスト エントリと同様に、エントリの順序は、順番に評価されるため、重要です。 IPv6 パケットがインターフェイスに到達すると、一致が見つかるまでアクセス リストの各エントリで、順に評価されます。

パケットが再帰許可エントリよりも前のエントリに一致した場合、そのパケットは、再帰許可エントリによって評価されず、再帰アクセス リストの一時エントリが作成されません（セッション フィルタリングはトリガーされません）。

パケットは、他の一致が先に発生しない場合にのみ、再帰許可エントリによって評価されます。 次に、パケットが再帰許可エントリで指定されたプロトコルに一致すると、パケットが転送され、対応する一時エントリが再帰アクセス リストに作成されます（そのパケットが進行中のセッションに属することを示す対応するエントリがまだ存在しない場合）。 一時エントリは、同じセッションでのみネットワークへのトラフィックを許可する条件を指定します。

再帰アクセス リスト エントリの特性

reflect キーワードを指定した **permit**（IPv6）コマンドは、**permit**（IPv6）コマンドで定義されている IPv6 再帰アクセス リストの一時エントリの作成をイネーブルにします。 一時エントリは、**permit**（IPv6）コマンドで指定されたプロトコルと、ネットワークから出て行く IPv6 パケットが一致するときに作成されます。 （パケットが、エントリの作成を「トリガー」します）。これらのエントリには次の特性があります。

- エントリは許可エントリです。
- エントリは元のトリガー パケットと同じ IP 上位層プロトコルを指定します。
- エントリは元のトリガー パケットと同じ送信元および宛先アドレスを指定します。ただし、これらのアドレスが入れ替わります。
- 元のトリガー パケットが TCP または UDP である場合、そのエントリは元のパケットと同じ送信元および宛先ポート番号を指定します。ただし、これらのポート番号が入れ替わります。
- 元のトリガー パケットが TCP または UDP 以外のプロトコルの場合、ポート番号は適用されず、他の条件が指定されます。 たとえば、ICMP の場合、タイプ番号が使用されます。一時エントリは元のパケットと同じタイプ番号を指定します（ただし、1 つだけ例外があり、元

の ICMP パケットがタイプ 8 の場合、一致する回帰 ICMP パケットはタイプ 0 である必要があります）。

- エントリは、上記 4 件の項目で示す例外を除き、元のトリガー パケットのすべての値を継承します。
- 内部ネットワークに入る IPv6 トラフィックは、エントリが期限切れになるまで、エントリに対して評価されます。 IPv6 パケットがエントリに一致した場合、パケットはネットワークに転送されます。
- エントリは、セッションの最後のパケットが照合された後に失効（または削除）されます。
- セッションに属するパケットが設定された時間（タイムアウト期間）検出されない場合、エントリは期限切れになります。

例

次の例では、OUTBOUND および INBOUND という名の IPv6 アクセス リスト 2 つを設定し、そのアクセス リストをイーサネット インターフェイス 0 上の発信および着信トラフィックに適用する方法を示します。 OUTBOUND リスト内の最初と 2 番めの許可エントリは、ネットワーク 2001:ODB8:0300:0201::/64 から送信されたすべての TCP および UDP パケットがイーサネット インターフェイス 0 から出て行くことを許可します。 また、エントリは REFLECTOUT という名前の一時的な IPv6 再帰アクセス リストを設定して、イーサネット インターフェイス 0 上で回帰（着信）TCP および UDP パケットをフィルタリングします。 OUTBOUND リストの最初の拒否エントリは、ネットワーク FEC0:0:0:0201::/64 から送信されたすべてのパケット（送信元 IPv6 アドレスの最初の 64 ビットとしてサイトローカル プレフィックス FEC0:0:0:0201 を持つパケット）がイーサネット インターフェイス 0 から出て行くことを拒否します。 OUTBOUND リストの 3 番めの許可エントリは、イーサネットインターフェイス 0 から出るすべての ICMP パケットを許可します。

INBOUND リストの許可エントリは、すべての ICMP パケットをイーサネット インターフェイス 0 で受信するのを許可します。 リストの **evaluate** コマンドは、REFLECTOUT という名前の一時的な IPv6 再帰アクセス リストをイーサネット インターフェイス 0 上の着信 TCP および UDP パケットに適用します。 OUTBOUND リストによって発信 TCP または UDP パケットがイーサネット インターフェイス 0 上で許可された場合、INBOUND リストは REFLECTOUT リストを使用して、回帰（着信）TCP および UDP パケットを照合（評価）します。 IPv6 ACL 内に IPv6 再帰アクセス リストをネストさせる方法の詳細については **evaluate** コマンドを参照してください。

```
ipv6 access-list OUTBOUND
 permit tcp 2001:0DB8:0300:0201::/64 any reflect REFLECTOUT
 permit udp 2001:0DB8:0300:0201::/64 any reflect REFLECTOUT
 deny FEC0:0:0:0201::/64 any
 permit icmp any any
ipv6 access-list INBOUND
 permit icmp any any
 evaluate REFLECTOUT
interface ethernet 0
 ipv6 traffic-filter OUTBOUND out
 ipv6 traffic-filter INBOUND in
```

（注） **permit any any** ステートメントが OUTBOUND または INBOUND アクセス リストの最後のエントリとして含まれていない場合、TCP、UDP、およびICMPパケットだけがイーサネットインターフェイス 0 の双方向（着信および発信）で許可されます（アクセス リストの末尾にある、暗黙の条件によりインターフェイス上のその他のパケット タイプはすべて拒否されます）。

次に、UDPトラフィック照合を許可する例を示します。 認証ヘッダーが存在する可能性があります。

```
permit udp any any sequence 10
```

次に、認証ヘッダーも存在する場合に、TCP トラフィックだけの照合を許可する例を示します。

```
permit tcp any any auth sequence 20
```

次に、認証ヘッダーが存在する場合に、任意の IPv6 トラフィックの照合を許可する例を示します。

```
permit ahp any any sequence 30
```

関連コマンド

コマンド	説明
deny（IPv6）	IPv6アクセスリストに拒否条件を設定します。
evaluate（IPv6）	IPv6 アクセス リスト内に IPv6 再帰アクセス リストをネストします。
ipv6 access-list	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ipv6 traffic-filter	インターフェイス上の着信または発信 IPv6 トラフィックをフィルタリングします。
show ipv6 access-list	現在のすべての IPv6 アクセス リストの内容を表示します。

prefix-glean

デバイスが IPv6 ルータ アドバタイズメント（RA）または Dynamic Host Configuration Protocol（DHCP）からプレフィックスを取り出せるようにするには、ipv6 スヌーピング コンフィギュレーション モードで **prefix-glean** コマンドを使用します。 これらのプロトコルのいずれかで収集したプレフィックスだけを学習し、残りを除外するには、このコマンドの **no** 形式を使用します。

prefix-glean [**only**]

no prefix-glean [**only**]

構文の説明

only	（任意）プレフィックスだけ収集します。

コマンド デフォルト

プレフィックスは RA または DHCP から学習されません。

コマンド モード

IPv6 スヌーピング コンフィギュレーション モード（config-ipv6-snooping）

コマンド履歴

リリース	変更内容
15.0(2)SE	このコマンドが導入されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

prefix-glean コマンドは、デバイスが RA および DHCP トラフィックでプレフィックスを学習できるようにします。

例

次に、デバイスがプレフィックスを学習できるようにする例を示します。

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# prefix-glean
```

関連コマンド

コマンド	説明
ipv6 snooping attach-policy	ターゲットに IPv6 スヌーピングにポリシーを適用します。
ipv6 snooping policy	IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング コンフィギュレーション モードを開始します。

protocol（IPv6）

アドレスを Dynamic Host Configuration Protocol（DHCP）またはネイバー探索プロトコル（NDP）で収集するように指定する、またはIPv6プレフィックス リストにプロトコルを関連付けるには、**protocol** コマンドを使用します。 DHCP または NDP によるアドレス収集をディセーブルにするには、このコマンドの **no** 形式を使用します。

protocol {**dhcp** | **ndp**} [**prefix-list** *prefix-list-name*]

no protocol {**dhcp** | **ndp**}

構文の説明

dhcp	アドレスを Dynamic Host Configuration Protocol（DHCP）パケットで取り出す必要があることを指定します。
ndp	アドレスをネイバー探索プロトコル（NDP）パケットで取り出す必要があることを指定します。
prefix-list *prefix-list-name*	（任意）保護されたプレフィックスのプレフィックス リストを使用することを指定します。

コマンド デフォルト

スヌーピングとリカバリは DHCP および NDP 両方を使用して試行されます。 プレフィックス リストは使用されず、すべてのアドレス範囲が受け入れられます。

コマンド モード

IPv6 スヌーピング コンフィギュレーション モード（config-ipv6-snooping）

コマンド履歴

リリース	変更内容
15.2(4)S	このコマンドが導入されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

アドレスが DHCP または NDP に関連付けられたプレフィックス リストと一致しなければ、制御パケットがドロップされ、バインディングテーブルエントリのリカバリはそのプロトコルでは試みられません。

- 指定されたプレフィックスリストがない場合、すべてのプロトコルがデフォルトでサポートされます。 チェックがないため、すべてのアドレスが受け入れられます。
- **no protocol** {**dhcp** | **ndp**} コマンドを使用すると、プロトコルがスヌーピングまたはグリーニングに使用されないことを示します。
- ただし、**no protocol dhcp** コマンドが使用されなければ、DHCP はまだバインディング テーブルのリカバリに使用できます。
- DHCP で取得されたアドレスが NDP によって確認される必要があるため、NDP プレフィックス リストは DHCP プレフィックス リストのスーパーセットである必要があります。
- プレフィックス リストが指定され、プロトコル パケットでそのプロトコルのプレフィックス リストに一致しないアドレスが示された場合、パケットはドロップされます（セキュリティ レベルが「glean」でない場合）。
- データのグリーニングは DHCP および NDP でリカバリできますが、宛先ガードは DHCP でのみリカバリします。

（注） **protocol** コマンドを設定する前に、プレフィックス リストを **ipv6 prefix-list** コマンドを使用して設定するときに、**ge** *ge-value* オプションの値を指定する必要があります。

例

次の例では、IPv6プレフィックスリスト（「abc」）の有効な設定を示し、DHCPを使用してプレフィックス リスト abc と一致したアドレスを回復します。

```
Device(config)# ipv6 prefix-list abc seq 5 permit 2001:DB8::/64 ge 128
!
Device(config-ipv6-snooping)# protocol dhcp prefix-list abc
```

関連コマンド

コマンド	説明
ipv6 prefix-list	IPv6 プレフィックス リストのエントリを作成します。
ipv6 snooping policy	IPv6スヌーピング コンフィギュレーション モードを開始します。

redistribute（IPv6）

あるルーティング ドメインから別のルーティング ドメインに IPv6 ルートを再配布するには、アドレス ファミリ コンフィギュレーション モードまたはルータ コンフィギュレーション モードで **redistribute** コマンドを使用します。 再配布をディセーブルにするには、このコマンドの **no** 形式を使用します。

redistribute source-protocol [*process-id*] [**include-connected** {**level-1**| **level-1-2**| **level-2**}] [*as-number*] [**metric** {*metric-value*| **transparent**}] [**metric-type** *type-value*] [**match** {**external** [**1**| **2**]| **internal**| **nssa-external** [**1**| **2**]}] [**tag** *tag-value*] [**route-map** *map-tag*]

no redistribute source-protocol [*process-id*] **[include-connected]** {**level-1**| **level-1-2**| **level-2**} [*as-number*] [**metric** {*metric-value*| **transparent**}] [**metric-type** *type-value*] [**match** {**external** [**1**| **2**]| **internal**| **nssa-external** [**1**| **2**]}] [**tag** *tag-value*] [**route-map** *map-tag*]

構文の説明

source-protocol	ルートの再配布元であるソース プロトコルです。 **bgp**、connected、**eigrp**、**isis**、**ospf**、**rip**、または **static** のキーワードのいずれかになります。
process-id	（任意）**bgp** または **eigrp** キーワードの場合、プロセス ID は 16 ビットの 10 進数であるボーダー ゲートウェイ プロトコル（BGP）の自律システム番号です。 **isis** キーワードの場合、プロセス ID はルーティング プロセスのわかりやすい名前を定義するオプションの値です。各ルータに指定できる IS-IS プロセスは 1 つだけです。 ルーティング プロセスの名前を作成することは、ルーティングを設定するときに名前を使用することを意味します。 **ospf** キーワードの場合、プロセス ID は、IPv6 ルーティング プロセスの Open Shortest Path First（OSPF）がイネーブルのときに管理上割り当てられる番号です。 **rip** キーワードの場合、プロセス ID は IPv6 Routing Information Protocol（RIP）ルーティング プロセスのわかりやすい名前を定義するオプションの値です。

include-connected	（任意）ソースプロトコルから学習したルートと、ソースプロトコルが動作しているインターフェイス上の接続先プレフィックスを、ターゲット プロトコルが再配布できるようにします。
level-1	Intermediate System-to-Intermediate System（IS-IS）用に、レベル 1 ルートが他の IP ルーティングプロトコルに個別に再配布されることを指定します。
level-1-2	IS-IS 用に、レベル 1 とレベル 2 の両方のルートが他の IP ルーティング プロトコルに再配布されることを指定します。
level-2	IS-IS 用に、レベル 2 ルートが他の IP ルーティングプロトコルに個別に再配布されることを指定します。
as-number	（任意）再配布ルートの自律システム番号。
metric *metric-value*	（任意）同じルータ上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。
metric transparent	（任意）RIP が、RIP メトリックとして再配布ルートのルーティング テーブル メトリックを使用します。

metric-type *type-value*	（任意）OSPF の場合、OSPF ルーティング ドメインにアドバタイズされるデフォルトのルートに関連付けられる外部リンク タイプを指定します。次の2つの値のいずれかにすることができます。 • **1**：タイプ 1 外部ルート • **2**：タイプ 2 外部ルート **metric-type** キーワードに値が指定されていない場合、Cisco IOS ソフトウェアは、タイプ 2 外部ルートを受け入れます。 IS-IS の場合、リンク タイプは次の 2 つの値のいずれかになります。 • **internal**：63 までの IS-IS メトリック。 • **external**:64 から 128 の IS-IS メトリック。 デフォルトは、**internal** です。
match {**external [1 | 2]**| **internal | nssa-external [1 | 2]**	（任意）OSPF では、ルートが match キーワードを使用して他のルーティング ドメインに再配布されます。これは次のいずれかで使用されます。 • **external [1 | 2]**：自律システム外部のルートである一方で、タイプ 1 またはタイプ 2 の外部ルートとして OSPF にインポートされているルート。 • **internal**：特定の自律システムの内部にあるルート。 • **nssa-external** [**1** | **2**]：自律システムの外部にあるが、Not So Stubby Area（NSSA）で OSPF for IPv6 にタイプ 1 またはタイプ 2 の外部ルートとしてインポートされているルート。

tag *tag-value*	（任意）各外部ルートに付加する 32 ビットの 10 進値を指定します。 これは OSPF 自体には使用されません。 自律システム境界ルータ（ASBR）間で情報を通信するために使用できます。 何も指定しない場合、BGP および外部ゲートウェイ プロトコル（EGP）からのルートにはリモート自律システムの番号が使用され、その他のプロトコルには 0 が使用されます。
route-map	（任意）このソース ルーティング プロトコルから現在のルーティング プロトコルへのルートのインポートをフィルタリングするために検査する必要のあるルート マップを指定します。 route-map キーワードが指定されない場合、すべてのルートが再配布されます。 このキーワードが指定されていて、ルート マップ タグがリストされていない場合、ルートはインポートされません。
map-tag	（任意）設定されたルート マップの ID。

コマンド デフォルト　ルートの再配布はディセーブルです。

コマンド モード　アドレス ファミリ コンフィギュレーション ルータ コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(15)T	このコマンドが導入されました。
12.4(6)T	Enhanced Interior Gateway Routing Protocol（EIGRP）IPv6 のサポートが追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

リリース	変更内容
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ ルータで追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

いずれかのキーワードを変更またはディセーブルにしても、他のキーワードの状態には影響しません。

内部メトリックを持つ IPv6 IS-IS ルートを受信するルータは、それ自身から再配布するルータまでのルートのコストと、アドバタイズされたコストの合計で、宛先に到達すると判断します。 外部メトリックでは、宛先に達するまでのアドバタイズされたコストだけを考慮します。

IS-IS は include-connected キーワードで設定されたルートの設定された再配布を無視します。 IS-IS は、IS-IS がインターフェイス上で実行されているか、インターフェイスがパッシブに設定されている場合、インターフェイスのプレフィックスをアドバタイズします。

IPv6 ルーティング プロトコルから学習したルートは、接続されたエリアにレベル 1 で IPv6 IS-IS に、またはレベル 2 で再配布できます。 **level-1-2** キーワードはレベル 1 とレベル 2 の両方のルートを 1 つのコマンドで許可します。

IPv6 RIP の場合、直接接続されたルートであるかのようにスタティック ルートをアドバタイズするには、**redistribute** コマンドを使用します。

注意 不適切に設定されている場合は、直接接続されたルートとしてスタティック ルートをアドバタイジングすると、ルーティング ループが発生する可能性があります。

再配布された IPv6 RIP ルーティング情報は、**distribute-list prefix-list** ルータ コンフィギュレーション コマンドによって常にフィルタリングする必要があります。 **distribute-list prefix-list** コマンドの使用により、管理者が意図するルートだけが、受信側のルーティング プロトコルに渡されることを保障します。

（注） IPv6 RIP の **redistribute** コマンドで指定された **metric** 値は、**default-metric** コマンドを使用して指定された **metric** 値よりも優先されます。

（注） IPv4では、プロトコルを再配布する場合、デフォルトでプロトコルが実行されているインターフェイスのサブネットも再配布されます。 IPv6 では、これはデフォルトの動作ではありません。 プロトコルが IPv6 で動作しているインターフェイスのサブネットを再配布するには、include-connected キーワードを使用します。 IPv6 では、この機能は、ソース プロトコルが BGP の場合はサポートされません。

redistribute コマンドが設定されていない場合、パラメータ設定は、クライアント プロトコルが IS-IS または EIGRP の場合は無視されます。

IS-IS 再配布は、IS-IS レベル 1 およびレベル 2 がユーザによって削除されると完全に削除されます。 IS-IS レベル設定は、redistribute コマンドだけを使用して設定できます。

すべてのルート タイプ値がユーザによって削除されると、デフォルトの再配布タイプは OSPF にリストアされます。

例

次の例では、IPv6 IS-IS の IPv6 BGP ルートを再配布するように設定します。 メトリックは 5 として指定され、メトリック タイプは、内部メトリックより優先順位が低いことを示す外部に設定されます。

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# redistribute bgp 64500 metric 5 metric-type external
```

次に、cisco という名前の IPv6 RIP ルーティング プロセスに IPv6 BGP ルートを再配布する例を示します。

```
Router(config)# ipv6 router rip cisco
Router(config-router)# redistribute bgp 42
```

次に、OSPF for IPv6 ルーティング プロセス 1 に IS-IS for IPv6 ルートを再配布する例を示します。

```
Router(config)# ipv6 router ospf 1
Router(config-router)# redistribute isis 1 metric 32 metric-type 1 tag 85
```

次の例では、ospf 1 がプレフィックス 2001:1:1::/64 および 2001:99:1::/64 と、rip 1 を通じて学習したプレフィックスを再配布します。

```
interface ethernet0/0
 ipv6 address 2001:1:1::90/64
 ipv6 rip 1 enable
interface ethernet1/1
 ipv6 address 2001:99:1::90/64
 ipv6 rip 1 enable
interface ethernet2/0
 ipv6 address 2001:1:2::90/64
 ipv6 ospf 1 area 1
ipv6 router ospf 1
  redistribute rip 1 include-connected
```

次の設定例および出力例は、最後のルート タイプ値を削除すると、redistribute コマンド パラメータがなくなることを示しています。

```
Router(config-router)# redistribute rip process1 metric 7
Router(config-router)# do show run | include redistribute
 redistribute rip process1 metric 7
Router(config-router)# no redistribute rip process1 metric 7
```

```
Router(config-router)# do show run | include redistribute
 redistribute rip process1
Router(config-router)#
```

関連コマンド

コマンド	説明
default-metric	再配布されるルートのデフォルト メトリックを指定します。
distribute-list prefix-list（IPv6 EIGRP）	インターフェイス上で受信または送信される EIGRP for IPv6 ルーティング アップデートに、プレフィックス リストを適用します。
distribute-list prefix-list（IPv6 RIP）	インターフェイス上で受信または送信される IPv6 RIP ルーティング アップデートに、プレフィックス リストを適用します。
redistribute isis（IPv6）	ターゲット プロトコルとソース プロトコルの両方として IS-IS を使用して、あるルーティング ドメインから別のルーティング ドメインに IPv6 ルートを再配布します。

router-preference maximum

アドバタイズされたデフォルト ルータ プリファレンス パラメータ値を確認するには、RA ガード ポリシー コンフィギュレーション モードで **router-preference maximum** コマンドを使用します。

router-preference maximum {**high**| **low**| **medium**}

構文の説明

high	デフォルト ルータ プリファレンス パラメータ値が指定された制限を超えています。
medium	デフォルト ルータ プリファレンス パラメータ値が指定された制限と同じです。
low	デフォルト ルータ プリファレンス パラメータ値が指定された制限よりも低くなっています。

コマンド デフォルト

ルータ プリファレンスの最大値は設定されていません。

コマンド モード

RA ガード ポリシー コンフィギュレーション（config-ra-guard）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.2(4)S	このコマンドが Cisco IOS Release 15.2(4)S に統合されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

router-preference maximum コマンドによって、アドバタイズされたデフォルト ルータ プリファレンス パラメータ値が指定された制限以下であることを確認できます。このコマンドは、トランク ポートでアドバタイズされるデフォルト ルータに低いプライオリティを指定し、アクセス ポートでアドバタイズされるデフォルト ルータを優先するために使用できます。

router-preference maximum コマンドの制限は、high、medium、low です。 たとえば、この値が **medium** に設定され、受信パケットのアドバタイズされたデフォルト ルータ プリファレンスが **high** に設定されている場合、パケットはドロップされます。受信パケットでコマンドオプションが **medium** または **low** に設定されている場合、パケットはドロップされません。

例

次に、ルータ アドバタイズメント（RA）ガード ポリシー名を raguard1 として定義し、ルータを RA ガード ポリシー コンフィギュレーション モードにして、router-preference maximum の検証を high に設定する例を示します。

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# router-preference maximum high
```

関連コマンド

コマンド	説明
ipv6 nd raguard policy	RA ガード ポリシー名を定義し、RA ガード ポリシー コンフィギュレーション モードを開始します。

ipv6-r1

- sec-level minimum, 187 ページ
- server name（IPv6 TACACS+）, 189 ページ
- show ipv6 access-list, 191 ページ
- show ipv6 dhcp conflict, 195 ページ
- show ipv6 interface, 197 ページ
- show ipv6 mld snooping, 207 ページ
- show ipv6 nd ra-throttle policy, 209 ページ
- show ipv6 nd ra-throttle vlan, 210 ページ
- show ipv6 nd raguard policy, 211 ページ
- show ipv6 neighbor binding, 213 ページ
- show ipv6 neighbors, 215 ページ
- show ipv6 protocols, 222 ページ
- show ipv6 route, 227 ページ
- show ipv6 snooping capture-policy, 233 ページ
- show ipv6 snooping counters, 235 ページ
- show ipv6 snooping features, 237 ページ
- show ipv6 snooping policies, 239 ページ
- show ipv6 traffic, 241 ページ
- summary-prefix（OSPFv3）, 245 ページ
- throttle-period, 248 ページ
- timers spf（IPv6）, 249 ページ
- timers throttle lsa, 251 ページ

- tracking, 253 ページ
- tunnel mode ipv6ip, 256 ページ
- vlan configuration, 262 ページ

sec-level minimum

暗号化生成アドレス（CGA）オプションを使用する場合の最小セキュリティ レベル パラメータ値を指定するには、ネイバー探索（ND）インスペクション ポリシー コンフィギュレーション モードで **sec-level minimum** コマンドを使用します。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

sec-level minimum *value*

no sec-level minimum *value*

構文の説明

value	1 ～ 7 の値で表す、最小限のセキュリティ レベル。 デフォルトのセキュリティ レベルは 1 です。 最も安全なレベルは 3 です。

コマンド デフォルト

デフォルトのセキュリティ レベルは 1 です。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション（config-nd-inspection）

RA ガード ポリシー コンフィギュレーション（config-ra-guard）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

sec-level minimum コマンドは、CGA オプションを使用する場合の最小セキュリティ レベル パラメータ値を指定します。 **sec-level minimum** コマンドは、**ipv6 nd inspection policy** コマンドを使用して ND インスペクション ポリシー コンフィギュレーション モードをイネーブルにした後で使用します。

例

次に、policy1 として ND ポリシー名を定義し、ルータを ND インスペクション ポリシー コンフィギュレーション モードにして、最小 CGA セキュリティ レベルとして 2 を指定する例を示します。

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# sec-level minimum 2
```

関連コマンド

コマンド	説明
ipv6 nd inspection policy	ND インスペクション ポリシー名を定義して、ND インスペクション ポリシー コンフィギュレーション モードを開始します。
ipv6 nd raguard policy	RA ガード ポリシー名を定義し、RA ガード ポリシー コンフィギュレーション モードを開始します。

server name（IPv6 TACACS+）

IPv6 TACACS+ サーバを指定するには、TACACS+ グループ サーバ コンフィギュレーション モードで **server name** コマンドを使用します。 コンフィギュレーションから IPv6 TACACS+ サーバを削除するには、このコマンドの **no** 形式を使用します。

server name *server-name*

no server name *server-name*

構文の説明

server-name	使用する IPv6 TACACS+ サーバ。

コマンド デフォルト

サーバ名は指定されていません。

コマンド モード

TACACS+ グループ サーバ コンフィギュレーション（config-sg-tacacs+）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2S	このコマンドが導入されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

このコマンドを設定する前に、**aaa group server tacacs** コマンドを設定します。

IPv6 TACACS+ サーバを指定するには、**server name** コマンドを入力します。

例

次に、server1 という名前の IPv6 TACACS+ サーバを指定する例を示します。

```
Router(config)# aaa group server tacacs+
Router(config-sg-tacacs+)# server name server1
```

関連コマンド

コマンド	説明
aaa group server tacacs	IPv6 または IPv4 の TACACS+ サーバを設定し、TACACS+ サーバ コンフィギュレーション モードを開始します。

show ipv6 access-list

現在のすべての IPv6 アクセス リストの内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 access-list** コマンドを使用します。

show ipv6 access-list [*access-list-name*]

構文の説明

access-list-name	（任意）アクセス リストの名前

コマンド デフォルト

すべての IPv6 アクセス リストが表示されます。

コマンド モード

ユーザ EXEC 特権 EXEC

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.0(23)S	プライオリティ フィールドがシーケンスに変更され、レイヤ4プロトコル情報（拡張 IPv6 アクセス リスト機能）が表示出力に追加されました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.2(50)SY	このコマンドが変更されました。 IPv4 および IPv6 ハードウェア統計情報に関する情報が表示されます。

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

IPv6 専用である点を除いて、**show ipv6 access-list** コマンドの出力は **show ip access-list** コマンドと類似しています。

例

次の例では、**show ipv6 access-list** コマンドで出力された inbound、tcptraffic、および outbound という名の IPv6 アクセス リストを示します。

```
Router# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
       left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
    (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

次の出力例は、IPSec で使用するための IPv6 アクセス リスト情報を示しています。

```
Router#  show ipv6 access-list
IPv6 access list Tunnel0-head-0-ACL (crypto)
     permit ipv6 any any (34 matches) sequence 1
IPv6 access list Ethernet2/0-ipsecv6-ACL (crypto)
     permit 89 FE80::/10 any (85 matches) sequence 1
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *1*：*show ipv6 access-list* のフィールドの説明

フィールド	説明
ipv6 access list inbound	IPv6 アクセス リスト名（例：inbound）。
permit	指定されたプロトコル タイプと一致するパケットを許可します。
tcp	伝送制御プロトコル。パケットが一致しなければならない高いレベル（レイヤ 4）のプロトコル タイプ。
any	::/0 と同じです。
eq	TCP または UDP パケットの送信元または宛先ポートを比較する equal オペランド。

フィールド	説明
bgp	ボーダー ゲートウェイ プロトコル。パケットが等しくなる必要がある低レベル（レイヤ 3）プロトコル タイプ。
reflect	再帰 IPv6 アクセス リストを示します。
tcptraffic (8 matches)	再帰 IPv6 アクセス リストの名前と、アクセス リストに一致した数。**clear ipv6 access-list** 特権 EXEC コマンドは、IPv6 アクセス リストの一致カウンタをリセットします。
sequence 10	着信パケットが比較されるアクセス リストの行のシーケンス。アクセス リストの行は、最初のプライオリティ（最低の数、たとえば 10）から最後のプライオリティ（最高の数、たとえば 80）の順に並んでいます。
host 2001:0DB8:1::1	パケットの送信元アドレスが一致する必要がある送信元 IPv6 ホスト アドレス。
host 2001:0DB8:1::2	パケットの宛先アドレスが一致する必要がある宛先 IPv6 ホスト アドレス。
11000	発信接続用の一時的な送信元ポート番号。
timeout 300	一時的な IPv6 再帰アクセス リスト tcptraffic が指定されたセッションをタイムアウトするまでのアイドル時間の間隔の合計（秒単位）。
(time left 243)	一時的な IPv6 再帰アクセス リスト tcptraffic が指定されたセッションを削除するまでのアイドル時間の合計（秒単位）。指定したセッションと一致するトラフィックを追加で受信すると、この値が 300 秒にリセットされます。
evaluate udptraffic	udptraffic という名前の IPv6 再帰アクセス リストが outbound という名前の IPv6 アクセス リスト内にネストされていることを示します。

関連コマンド

コマンド	説明
clear ipv6 access-list	IPv6 アクセス リストの一致カウンタをリセットします。
hardware statistics	ハードウェア統計情報の収集をイネーブルにします。
show ip access-list	現在のすべての IP アクセス リストの内容を表示します。
show ip prefix-list	プレフィックス リストまたはプレフィックス リスト エントリに関する情報を表示します。
show ipv6 prefix-list	IPv6 プレフィックス リストまたは IPv6 プレフィックスリストのエントリに関する情報を表示します。

show ipv6 dhcp conflict

アドレスをクライアントに提供するときに、Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバで見つかったアドレス競合を表示するには、特権 EXEC モードで **show ipv6 dhcp conflict** コマンドを使用します。

show ipv6 dhcp conflict [*ipv6-address*] [**vrf** *vrf-name*]

構文の説明

ipv6-address	（任意）IPv6 用 DHCP クライアントのアドレス。
vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.4(24)T	このコマンドが導入されました。
Cisco IOS XE Release 2.5	このコマンドが、Cisco IOS XE Release 2.5 に統合されました。
15.1(2)S	このコマンドが変更されました。 キーワードおよび引数 **vrf** *vrf-name* が追加されました。
Cisco IOS XE リリース 3.3S	このコマンドが変更されました。 キーワードおよび引数 **vrf** *vrf-name* が追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

競合を検出するように DHCPv6 サーバを設定する場合、DHCPv6 サーバは ping を使用します。 クライアントはネイバー探索を使用してクライアントを検出し、DECLINE メッセージを介してサーバに報告します。 アドレス競合が検出されると、このアドレスはプールから削除されます。管理者がこのアドレスを競合リストから削除するまでこのアドレスは割り当てることができません。

例

次に、**show ipv6 dhcp conflict** コマンドの出力例を示します。 このコマンドは、DHCP 競合のプール値とプレフィックス値を示します。

```
Router# show ipv6 dhcp conflict
Pool 350, prefix 2001:0DB8:1005::/48
     2001:0DB8:1005::10
```

関連コマンド

コマンド	説明
clear ipv6 dhcp conflict	DHCPv6 サーバデータベースからアドレス競合をクリアします。

show ipv6 interface

IPv6 用に設定されたインターフェイスの使用可能性ステータスを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 interface** コマンドを使用します。

show ipv6 interface [brief] [*type number*] **[prefix]**

構文の説明

brief	（任意）各インターフェイスの IPv6 ステータスおよびコンフィギュレーションの要約を表示します。
type	（任意）情報を表示するインターフェイス タイプ。
number	（任意）情報を表示するインターフェイス番号。
prefix	（任意）ローカルの IPv6 プレフィックス プールから生成されるプレフィックス。

コマンド デフォルト

すべての IPv6 インターフェイスが表示されます。

コマンド モード

ユーザ EXEC 特権 EXEC

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.2(4)T	OK、TENTATIVE、DUPLICATE、ICMP redirects、および ND DAD フィールドがコマンド出力に追加されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。

リリース	変更内容
12.2(25)S	コマンド出力が、現在のユニキャスト RPF の設定情報を表示するように更新されました。
12.4(2)T	コマンド出力が、インターフェイスを介してデバイスによってアドバタイズされるデフォルトルータプリファレンス（DRP）のプリファレンス値のステータスを表示するように更新されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.4(4)T	コマンド出力が、IPv6 のホットスタンバイ ルータ プロトコル（HSRP）情報を表示するように更新されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ デバイスで追加されました。
12.4(24)T	コマンド出力が、Dynamic Host Configuration Protocol（DHCP）から送信されたアドレスを表示するように更新されました。
12.2(50)SY	このコマンドが、Cisco IOS Release 12.2(50)SY に統合されました。
15.0(1)SY	このコマンドが、Cisco IOS Release 15.0(1)SY に統合されました。
15.2(2)SNG	このコマンドが、Cisco ASR 901 シリーズのアグリゲーション サービス デバイスに実装されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

show ipv6 interface コマンドの出力は、IPv6 に固有である点を除き、show ip interface コマンドの出力と似ています。

インターフェイスの IPv6 ステータスおよび設定されたアドレスを確認するには、**show ipv6 interface** コマンドを使用します。 show ipv6 interface コマンドは、IPv6 がこのインターフェイスおよび設定済みの機能の操作に使用しているパラメータも表示します。

インターフェイスのハードウェアが使用できる場合、インターフェイスはupとマークされます。インターフェイスが IPv6 用の双方向通信を提供できる場合、回線プロトコルは up とマークされます。

オプションのインターフェイス タイプおよび番号を指定すると、その特定のインターフェイスに関する情報だけが表示されます。 特定のインターフェイスについて、インターフェイスで設定された IPv6 ネイバー探索（ND）プレフィックスを表示するには、prefix キーワードを入力します。

例

例

show ipv6 interface コマンドは、指定されたインターフェイスに関する情報を表示します。

```
Device(config)# show ipv6 interface ethernet0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:6700
  No Virtual link-local address(es):
  Global unicast address(es):
    2001::1, subnet is 2001::/64 [DUP]
    2001::A8BB:CCFF:FE00:6700, subnet is 2001::/64 [EUI]
    2001:100::1, subnet is 2001:100::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF00:6700
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *2*：***show ipv6 interface*** のフィールドの説明

フィールド	説明
Ethernet0/0 is up, line protocol is up	インターフェイス ハードウェアがアクティブかどうか（回線信号が存在するかどうか）、およびそれが管理者によりダウン状態にされているかどうかを示します。 インターフェイス ハードウェアが使用可能な場合、インターフェイスは「up」とマークされます。インターフェイスが使用可能になるには、インターフェイス ハードウェアと回線プロトコルの両方がアップ状態になければなりません。

フィールド	説明
line protocol is up、down（down は、出力例では示されていません）	回線プロトコルを処理するソフトウェアプロセスが回線を使用可能とするかどうか（つまり、キープアライブが成功しているかどうか、またはIPv6 CPがネゴシエートされているかどうか）を示します。インターフェイスが双方向通信を提供できる場合、回線プロトコルは up とマークされます。インターフェイスが使用可能であるためには、インターフェイスハードウェアと回線プロトコルの両方がアップ状態である必要があります。
IPv6 is enabled, stalled, disabled (ストールまたはディセーブルについては、出力例では示されていません)	IPv6がインターフェイスでイネーブル、ストールまたはディセーブルかを示します。 IPv6 がイネーブルの場合、インターフェイスは「enabled」とマークされます。重複アドレス検出処理がインターフェイスのリンクローカルアドレスを重複アドレスと識別した場合、IPv6パケットは、そのインターフェイスでディセーブルであり、インターフェイスは「stalled」とマークされます。IPv6がイネーブルでない場合、インターフェイスは「disabled」とマークされます。
link-local address	インターフェイスに割り当てられているリンクローカル アドレスを表示します。
Global unicast address(es):	インターフェイスに割り当てられているグローバル ユニキャスト アドレスを表示します。
Joined group address(es):	このインターフェイスが属するマルチキャストグループを示します。
MTU	インターフェイスの最大伝送単位。
ICMP error messages	このインターフェイス上で送信されるエラーメッセージ間の最小間隔をミリ秒で指定します。
ICMP redirects	インターフェイスでのインターネット制御メッセージ プロトコル（ICMP）IPv6 リダイレクトメッセージの状態（メッセージの送信かイネーブルかディセーブルか）。

フィールド	説明
ND DAD	インターフェイスでの重複アドレス検出の状態（イネーブルまたはディスーブル）。
number of DAD attempts:	重複アドレス検出が実行されているときに、インターフェイスで送信されるネイバー送信要求メッセージの連続数。
ND reachable time	このインターフェイスに割り当てられているネイバー探索到達可能時間（ミリ秒）を表示します。
ND advertised reachable time	このインターフェイスでアドバタイズされるネイバー探索到達可能時間（ミリ秒）を表示します。
ND advertised retransmit interval	このインターフェイスでアドバタイズされるネイバー探索再送信間隔（ミリ秒）を表示します。
ND router advertisements	このインターフェイスで送信されるネイバー探索ルータアドバタイズメント（RA）の間隔（秒単位）およびアドバタイズメントが期限切れになるまでの時間数を指定します。 Cisco IOS Release 12.4(2)T 以降では、このインターフェイスのこのデバイスから送信されるデフォルト ルータ プリファレンス（DRP）値を表示します。
ND advertised default router preference is Medium	特定のインターフェイス上のデバイスの DRP。

例

show ipv6 interface コマンドは、インターフェイスに割り当てられている IPv6 アドレスに関連付けることができる属性の情報を表示します。

属性	説明
ANY	エニーキャスト。 アドレスは、**ipv6 address** コマンドを使用して設定したときの指定どおり、エニーキャスト アドレスです。
CAL	カレンダー。 アドレスは時限制で、有効な推奨ライフタイムがあります。

属性	説明
DEP	非推奨。 時限アドレスは非推奨です。
DUP	重複。 アドレスは、重複アドレス検出（DAD）で判断されたとおり、重複しています。 DAD を再試行するには、インターフェイスで **shutdown** または **no shutdown** コマンドを使用する必要があります。
EUI	EUI-64 ベース。 アドレスは EUI-64 を使用して収集されました。
OFF	オフリンク。 アドレスは、オフリンクです。
OOD	Overly Optimistic DAD。 このアドレスに対しては DAD は実行されません。 この属性は仮想アドレスに適用されます。
PRE	優先。 時限アドレスが優先されます。
TEN	一時的。 アドレスは、DAD ごとに一時的な状態です。
UNA	非アクティブ。仮想アドレスはアクティブではなく、スタンバイ状態です。
VIRT	仮想。アドレスは仮想で、HSRP、VRRP、または GLBP によって管理されます。

次に、**brief** キーワードを入力した **show ipv6 interface** コマンドの出力例を示します。

```
Device# show ipv6 interface brief
Ethernet0 is up, line protocol is up
Ethernet0                  [up/up]
    unassigned
Ethernet1                  [up/up]
    2001:0DB8:1000:/29
Ethernet2                  [up/up]
    2001:0DB8:2000:/29
Ethernet3                  [up/up]
    2001:0DB8:3000:/29
Ethernet4                  [up/down]
    2001:0DB8:4000:/29
Ethernet5                  [administratively down/down]
    2001:123::210:7BFF:FEC2:ACD8
Interface         Status                IPv6 Address
Ethernet0         up                    3FFE:C00:0:1:260:3EFF:FE11:6770
Ethernet1         up                    unassigned
Fddi0             up                    3FFE:C00:0:2:260:3EFF:FE11:6772
Serial0           administratively down unassigned
Serial1           administratively down unassigned
Serial2           administratively down unassigned
```

```
Serial3           administratively down unassigned
Tunnel0           up                     unnumbered (Ethernet0)
Tunnel1           up                     3FFE:700:20:1::12
```

例

この出力例では、ローカル IPv6 プレフィックス プールからプレフィックスを生成したインターフェイスの特性を示します。

```
Device# show ipv6 interface Ethernet 0/0 prefix

interface Ethernet0/0
 ipv6 address 2001:0DB8::1/64
 ipv6 address 2001:0DB8::2/64
 ipv6 nd prefix 2001:0DB8:2::/64
 ipv6 nd prefix 2001:0DB8:3::/64 2592000 604800 off-link
end
.
.
.
IPv6 Prefix Advertisements Ethernet0/0
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default
       N - Not advertised, C - Calendar
     default [LA] Valid lifetime 2592000, preferred lifetime 604800
AD   2001:0DB8:1::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
APD  2001:0DB8:2::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
P    2001:0DB8:3::/64 [A] Valid lifetime 2592000, preferred lifetime 604800
```

デフォルト プレフィックスは ipv6 nd prefix default コマンドを使用して設定されるパラメータを示しています。

例

この出力例は、インターフェイス経由でこのデバイスによってアドバタイズされる DRP プリファレンス値の状態を示しています。

```
Device# show ipv6 interface gigabitethernet 0/1
  GigabitEthernet0/1 is up, line protocol is up
    IPv6 is enabled, link-local address is FE80::130
    Description: Management network (dual stack)
    Global unicast address(es):
      FEC0:240:104:1000::130, subnet is FEC0:240:104:1000::/64
    Joined group address(es):
      FF02::1
      FF02::2
      FF02::1:FF00:130
    MTU is 1500 bytes
    ICMP error messages limited to one every 100 milliseconds
    ICMP redirects are enabled
    ND DAD is enabled, number of DAD attempts: 1
    ND reachable time is 30000 milliseconds
    ND advertised reachable time is 0 milliseconds
    ND advertised retransmit interval is 0 milliseconds
    ND router advertisements are sent every 200 seconds
    ND router advertisements live for 1800 seconds
    ND advertised default router preference is Low
    Hosts use stateless autoconfig for addresses.
```

例

インターフェイスで HSRP IPv6 を初めて設定するとき、インターフェイスの IPv6 リンクローカル アドレスはアドバタイズされなくなるため、非アクティブ（UNA）にマークされます。また、HSRP IPv6 仮想リンクローカル アドレスが、UNA 属性と一時的な DAD（TEN）属性が設定され

て仮想リンクローカル アドレス リストに追加されます。 さらに、HSRP IPv6 マルチキャスト アドレスをリッスンするようにインターフェイスがプログラムされます。

この出力例では、HSRP IPv6 がインターフェイスで設定されるときの UNA および TEN 属性のステータスが表示されています。

```
Device# show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80:2::2 [UNA]
  Virtual link-local address(es):
    FE80::205:73FF:FEA0:1 [UNA/TEN]
  Global unicast address(es):
    2001:2::2, subnet is 2001:2::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::66
    FF02::1:FF00:2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ND DAD is enabled, number of DAD attempts: 1
```

HSRP グループがアクティブになると、UNA および TEN 属性はクリアされ、Overly Optimistic DAD（OOD）属性が設定されます。 HSRP 仮想 IPv6 アドレスの送信要求ノード マルチキャスト アドレスもインターフェイスに追加されます。

この出力例では、HSRP グループがアクティブになったときの UNA、TEN、および OOD 属性のステータスが表示されています。

```
Device# show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80:2::2 [UNA]
  Virtual link-local address(es):
    FE80::205:73FF:FEA0:1 [OPT]
  Global unicast address(es):
    2001:2::2, subnet is 2001:2::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::66
    FF02::1:FF00:2
    FF02::1:FFA0:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
```

次の表で、HSRP が設定されているときに **show ipv6 interface** コマンドで表示される追加の重要なフィールドについて説明します。

表 *3*：*HSRP* が設定されているときの *show ipv6 interface* コマンドのフィールドの説明

フィールド	説明
IPv6 is enabled, link-local address is FE80:2::2 [UNA]	インターフェイスの IPv6 リンクローカル アドレスはアドバタイズされないため、UNA にマークされます。
FE80::205:73FF:FEA0:1 [UNA/TEN]	UNA および TEN 属性が設定された仮想リンクローカル アドレス リスト。

フィールド	説明
FF02::66	HSRP IPv6 マルチキャスト アドレス。
FE80::205:73FF:FEA0:1 [OPT]	HSRP はアクティブになり、HSRP 仮想アドレスは OPT にマークされます。
FF02::1:FFA0:1	HSRP 送信要求ノード マルチキャスト アドレス。

例

インターフェイスでモバイルIPv6をイネーブルにすると、IPv6ルータアドバタイズメント（RA）の最小送信間隔を設定できます。 設定されている場合、**show ipv6 interface** コマンドの出力で最小 RA 間隔がレポートされます。 最小 RA 間隔が明示的に設定されていない場合、表示されません。

次の例では、イーサネット インターフェイス 1/0 で最大 RA 間隔が 100 秒に設定され、最小 RA 間隔が 60 秒として設定されています。

```
Device(config-if)# ipv6 nd ra-interval 100 60
```

その後、**show ipv6 interface** を使用すると、間隔は次のように表示されます。

```
Device(config)# show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 60 to 100 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

次の例では、イーサネットインターフェイス1/0で最大RA間隔が100ミリ秒（ms）に設定され、最小 RA 間隔が 60 ミリ秒として設定されています。

```
Device(config)# show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
```

```
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 60 to 100 milliseconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
```

次の表で、最小RA間隔情報が設定されているときに**show ipv6 interface**コマンドで表示される追加の重要なフィールドについて説明します。

表 *4*：最小 *RA* 間隔情報が設定されているときの *show ipv6 interface* コマンドのフィールドの説明

フィールド	説明
ND ルータ アドバタイズメントは 60 ～ 100 秒ごとに送信されます。	ND RA は最小値と最大値の間の値からランダムに選ばれた間隔で送信されます。 この例では、最小値は 60 秒で、最大値は 100 秒です。
ND ルータ アドバタイズメントは 60 ～ 100 ミリ秒ごとに送信されます。	ND RA は最小値と最大値の間の値からランダムに選ばれた間隔で送信されます。 この例では、最小値は60ミリ秒、最大値は100ミリ秒です。

関連コマンド

コマンド	説明
ipv6 nd prefix	IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定します。
ipv6 nd ra interval	インターフェイス上の IPv6 RA 送信間隔を設定します。
show ip interface	IP用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。

show ipv6 mld snooping

マルチキャスト リスナー検出バージョン 2（MLDv2）スヌーピング情報を表示するには、特権 EXEC モードで **show ipv6 mld snooping** コマンドを使用します。

show ipv6 mld [**vrf** *vrf-name*] **snooping** {**explicit-tracking vlan** *vlan*| **mrouter** [**vlan** *vlan*]| **report-suppression vlan** *vlan*| **statistics vlan** *vlan*}

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
explicit-tracking vlan *vlan*	明示的ホスト トラッキングのステータスを表示します。
mrouter	オプションの VLAN 上のマルチキャスト ルータ インターフェイスを表示します。
vlan *vlan*	（任意）マルチキャスト ルータ インターフェイス上の VLAN 番号を指定します。
report-suppression vlan *vlan*	レポート抑制のステータスを表示します。
statistics vlan *vlan*	VLAN 上の MLD スヌーピング情報を表示します。

コマンド デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(18)SXE	このコマンドが Supervisor Engine 720 に導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
15.1(4)M	キーワードおよび引数 **vrf** *vrf-name* が追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

引数を指定せずに **show ipv6 mld snooping mrouter** コマンドを入力すると、すべてのマルチキャスト ルータ インターフェイスを表示することができます。

例

次に、VLAN 25 の明示的トラッキング情報を表示する例を示します。

```
Router# show ipv6 mld snooping explicit-tracking vlan 25
Source/Group                    Interface    Reporter        Filter_mode
-------------------------------------------------------------------------
10.1.1.1/226.2.2.2              Vl25:1/2     10.27.2.3       INCLUDE
10.2.2.2/226.2.2.2              Vl25:1/2     10.27.2.3       INCLUDE
```

次に、VLAN 1 のマルチキャスト ルータ インターフェイスを表示する例を示します。

```
Router# show
ipv6 mld snooping mrouter vlan 1
vlan            ports
-----+---------------------------------------
  1          Gi1/1,Gi2/1,Fa3/48,Router
```

次に、VLAN 25 の MLD スヌーピング統計情報を表示する例を示します。

```
Router# show ipv6 mld
 snooping statistics interface vlan 25
Snooping staticstics for Vlan25
#channels:2
#hosts   :1

Source/Group            Interface       Reporter      Uptime        Last-Join   Last-Leave
10.1.1.1/226.2.2.2      Gi1/2:Vl25      10.27.2.3     00:01:47      00:00:50      -
10.2.2.2/226.2.2.2      Gi1/2:Vl25      10.27.2.3     00:01:47      00:00:50      -
```

関連コマンド

コマンド	説明
ipv6 mld snooping	MLDv2 スヌーピングをグローバルにイネーブルにします。
ipv6 mld snooping explicit-tracking	明示的なホスト トラッキングをイネーブルにします。
ipv6 mld snooping querier	MLDv2 スヌーピング クエリアをイネーブルにします。
ipv6 mld snooping report-suppression	VLAN 上でレポート抑制をイネーブルにします。

show ipv6 nd ra-throttle policy

IPv6 ルータ アドバタイズメント（RA）スロットル ポリシーに関する情報を表示するには、特権 EXEC モードで **show ipv6 nd ra-throttle policy** コマンドを使用します。

show ipv6 nd ra-throttle policy *policy-name*

構文の説明

policy-name	RA スロットル ポリシー名。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

トラブルシューティング用に IPv6 RA スロットル情報を表示するには、**show ipv6 nd ra-throttle policy** を使用します。

例

```
Device# show ipv6 nd ra-throttle policy policy2

Policy policy2 configuration:
        The throttle period will be coalesced and default to 600 seconds
        Applied to a port, this policy indicates a wired interface
        The maximum number of unthrottled RAs is configured on the vlan and defaults to 10
       The min and max numbers of unthrottled RAs per device will be coalesced and default
 to 10
      The behaviour upon RAs with an RFC 3775 interval option will be coalesced and default
 to passthrough

Policy applied on the following interfaces:
  Et0/0                vlan all
Policy applied on the following vlans:
  10,12-17
```

show ipv6 nd ra-throttle vlan

VLAN の IPv6 ルータ アドバタイズメント（RA）スロットル ポリシーのアクションに関する情報を表示するには、特権 EXEC モードで **show ipv6 nd ra-throttle vlan** コマンドを使用します。

show ipv6 nd ra-throttle vlan *vlan-id*[**advertising-routers**| **pending-hosts**]

構文の説明

vlan-id	VLAN または VLAN のコレクション。
advertising-routers	（任意）RA を最近発行したデバイスに関する情報を表示します。
pending-hosts	（任意）RA を待機している無線ホストに関する情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

VLAN の IPv6 RA スロットル ポリシーのアクションに関する情報を表示するには、**show ipv6 nd ra-throttle vlan** コマンドを使用します。

例

```
Device# show ipv6 nd ra-throttle vlan vlan1

general information for vlan1
---------------------------------

 RAs             last period     this period    overall
 passed_through  1               1              2
 throttled       4               2              6

 no pending host

current policy is tutu coalesced as:

  throttle-period 90 seconds remaining 48
  max-through 0
  allow at-least 1 at-most 1
  interval-option passthrough
```

show ipv6 nd raguard policy

RA ガード機能が設定されているすべてのインターフェイスのルータ アドバタイズメント（RA）ガード ポリシーを表示するには、特権 EXEC モードで **show ipv6 nd raguard policy** コマンドを使用します。

show ipv6 nd raguard policy [*policy-name*]

構文の説明

policy-name	（任意）RA ガード ポリシー名。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.2(4)S	このコマンドが Cisco IOS Release 15.2(4)S に統合されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

show ipv6 nd raguard policy コマンドは、RA ガード機能が設定されたすべてのインターフェイスのポリシーに設定されているオプションを表示します。

例

次の例では、raguard1 という名前のポリシーおよびポリシーが適用されているすべてのインターフェイスのポリシー設定を表示します。

```
Router# show ipv6 nd raguard policy interface raguard1

Policy raguard1 configuration:
  device-role host
Policy applied on the following interfaces:
  Et0/0        vlan all
  Et1/0        vlan all
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *5* : ***show ipv6 nd raguard policy*** のフィールドの説明

フィールド	説明
Policy raguard1 configuration:	指定されたポリシーの設定。
device-role host	ポートに接続されているデバイスのロール。このデバイス設定はホストの設定です。
Policy applied on the following interfaces:	RA ガード機能が設定されている特定のインターフェイス。

show ipv6 neighbor binding

バインディング テーブルの内容を表示するには、特権 EXEC モードで **show ipv6 neighbor binding** コマンドを使用します。

show ipv6 neighbor binding [**vlan** *vlan-id*| **interface** *type number*| **ipv6** *ipv6-address*| **mac** *mac-address*]

構文の説明

vlan *vlan-id*	（任意）指定したVLANに一致するバインディング テーブル エントリを表示します。
interface *type number*	（任意）指定したインターフェイス タイプおよび番号に一致するバインディング テーブル エントリを表示します。
ipv6 *ipv6-address*	（任意）指定された IPv6 アドレスに一致するバインディング テーブル エントリを表示します。
mac *mac-address*	（任意）指定されたメディア アクセス コントロール（MAC）アドレスに一致するバインディング テーブル エントリを表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

show ipv6 neighbor binding コマンドは、バインディング テーブルの内容を表示します。 表示出力は、特定の VLAN、インターフェイス、IPv6 アドレス、または MAC アドレスで指定できます。

キーワードまたは引数を入力しないと、すべてのバインディング テーブルの内容が表示されます。

次のキーワードと引数の組み合わせを使用できます。

- **vlan** *vlan-id*：指定された VLAN のすべてのエントリを表示します。
- **interface** *type number*：指定されたインターフェイスのすべてのエントリを表示します。
- **ipv6** *ipv6-address* + **interface** *type number* + **vlan** *vlan-id*：この 3 個のキーワードと引数の組み合わせに一致する 1 つのエントリを表示します。
- **ipv6** *ipv6-address* + **interface** *type number*：指定された IPv6 アドレスおよびインターフェイスのすべてのエントリを表示します。
- **ipv6** *ipv6-address*：指定された IPv6 アドレスのエントリを表示します。

例

次に、バインディング テーブルの内容を表示する例を示します。

```
Router# show ipv6 neighbor binding

address DB has 4 entries
Codes: L - Local, S - Static, ND - Neighbor Discovery
Preflevel (prlvl) values:
1:Not secure          2:MAC and LLA match   3:Cga authenticated
4:Dhcp assigned       5:Cert authenticated  6:Cga and Cert auth
7:Trusted port        8:Statically assigned
    IPv6 address            Link-Layer addr Interface   vlan  prlvl age state    Time left
ND  FE80::A8BB:CCFF:FE01:F500  AABB.CC01.F500  Et0/0     100  0002    0 REACHABLE  8850
L   FE80::21D:71FF:FE99:4900   001D.7199.4900  Vl100     100  0080 7203 DOWN       N/A
ND  2001:600::1                AABB.CC01.F500  Et0/0     100  0003    0 REACHABLE  3181
ND  2001:300::1                AABB.CC01.F500  Et0/0     100  0007    0 REACHABLE  9559
ND  2001:100::2                AABB.CC01.F600  Et1/0     200  0002    0 REACHABLE  9196
L   2001:400::1                001D.7199.4900  Vl100     100  0080 7188 DOWN       N/A
S   2001:500::1                000A.000B.000C  Fa4/13    300  0080 8676 STALE      N/A
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *6*：*show ipv6 neighbor binding* のフィールドの説明

フィールド	説明
address DB has *n* entries	指定されたデータベースのエントリ数。

関連コマンド

コマンド	説明
ipv6 neighbor binding	バインディングテーブルのネイバーバインディング エントリのデフォルトを変更します。

show ipv6 neighbors

IPv6 ネイバー探索（ND）キャッシュ情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 neighbors** コマンドを使用します。

show ipv6 neighbors [*interface-type interface-number*| *ipv6-address*| *ipv6-hostname*| **statistics**]

構文の説明

interface-type	（任意）IPv6 ネイバー情報を表示するインターフェイスのタイプを指定します。
interface-number	（任意）IPv6 ネイバー情報を表示するインターフェイスの番号を指定します。
ipv6-address	（任意）ネイバーの IPv6 アドレスを指定します。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
ipv6-hostname	（任意）リモート ネットワーキング デバイスの IPv6 ホスト名を指定します。
statistics	（任意）ND キャッシュ統計情報を表示します。

コマンド デフォルト

すべての IPv6 ND キャッシュ エントリを一覧表示します。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.2(8)T	このコマンドが変更されました。 IPv6 ネイバー探索キャッシュのスタティック エントリのサポートがコマンド出力に追加されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。

リリース	変更内容
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合され、Cisco ASR 1000 シリーズ デバイスで導入されました。
Cisco IOS XE Release 2.6	このコマンドが変更されました。このコマンドは、特定のインターフェイスのNDキャッシュエントリの数と制限を表示するように更新されました。
15.1(3)T	このコマンドが Cisco IOS Release 15.1(3)T に統合されました。
15.2(2)SNG	このコマンドが、Cisco ASR 901 シリーズのアグリゲーション サービス デバイスに実装されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

interface-type および *interface-number* 引数が指定されていない場合、すべての IPv6 ネイバーのキャッシュ情報が表示されます。 *interface-type* および *interface-number* 引数を指定すると、指定されたインターフェイスのキャッシュ情報だけが表示されます。

statistics キーワードを指定すると、ND キャッシュ統計情報が表示されます。

例

次に、インターフェイス タイプおよび番号を指定して入力された **show ipv6 neighbors** コマンドの出力例を示します。

```
Device# show ipv6 neighbors ethernet 2
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH Ethernet2
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e  REACH Ethernet2
3001:1::45a                                 - 0002.7d1a.9472  REACH Ethernet2
```

次に、IPv6 アドレスを指定して入力された **show ipv6 neighbors** コマンドの出力例を示します。

```
Device# show ipv6 neighbors 2000:0:0:4::2
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH Ethernet2
```

下の表で、ここで表示される重要なフィールドについて説明します。

表 *7*：*show ipv6 neighbors* のフィールドの説明

フィールド	説明
IPv6 Address	隣接またはインターフェイスの IPv6 アドレス。
Age	アドレスが到達可能と確認されてから経過した時間（分）。 ハイフン（-）はスタティック エントリを示します。
Link-layer Addr	MAC アドレス。 アドレスが不明の場合、ハイフン（-）が表示されます。

フィールド	説明
State	

フィールド	説明
	隣接キャッシュ エントリの状態。 次に、IPv6 ネイバー探索キャッシュのダイナミック エントリの状態を示します。 • INCMP（不完全）：エントリに対してアドレス解決を実行中です。 ネイバー送信要求メッセージがターゲットの送信要求ノード マルチキャスト アドレスに送信されましたが、対応するネイバー アドバタイズメント メッセージが受信されていません。 • REACH（到達可能）：ネイバーへの転送パスが正常に機能していることを示す肯定確認が、直近の ReachableTime ミリ秒以内に受信されました。 REACH 状態になっている間は、パケットが送信されるときにデバイスは特別なアクションを実行しません。 • STALE：転送パスが正常に機能していることを示す最後の肯定確認を受信してから ReachableTime ミリ秒を超える時間が経過しました。 STALE 状態になっている間は、パケットが送信されるまでデバイスはアクションを実行しません。 • DELAY：転送パスが正常に機能していることを示す最後の肯定確認を受信してから ReachableTime ミリ秒を超える時間が経過しました。 パケットは直近の DELAY_FIRST_PROBE_TIME 秒以内に送信されました。 DELAY 状態に入ってから、DELAY_FIRST_PROBE_TIME 秒以内に到達可能性確認を受信できない場合は、ネイバー送信要求メッセージが送信され、状態が PROBE に変更されます。 • PROBE：到達可能性確認が受信されるまで、RetransTimer ミリ秒ごとにネイバー送信要求メッセージを再送信して、到達可能性確認をアクティブに要求します。 • ????：不明状態 次に、IPv6 ネイバー探索キャッシュのスタ

フィールド	説明
	ティック エントリの可能な状態を示します。 • INCMP（不完全）：このエントリのインターフェイスはダウンしています。 • REACH（到達可能）：このエントリのインターフェイスは動作しています。 （注） 到達可能性検出は IPv6 ネイバー探索キャッシュのスタティック エントリに適用されないため、INCMP（不完全）状態と REACH（到達可能）状態の記述は、ダイナミック キャッシュ エントリとスタティック キャッシュ エントリで異なります。
Interface	アドレスに到達可能であったインターフェイス。

次に、**statistics** キーワードを指定した **show ipv6 neighbors** コマンドの出力例を示します。

```
Device# show ipv6 neighbor statistics

IPv6 ND Statistics
 Entries 2, High-water 2, Gleaned 1, Scavenged 0
 Entry States
   INCMP 0  REACH 0  STALE 2  GLEAN 0  DELAY 0  PROBE 0
 Resolutions (INCMP)
   Requested 1, timeouts 0, resolved 1, failed 0
   In-progress 0, High-water 1, Throttled 0, Data discards 0
 Resolutions (PROBE)
   Requested 3, timeouts 0, resolved 3, failed 0
```

下の表で、ここで表示される重要なフィールドについて説明します。

表 *8*：*show ipv6 neighbors statistics* のフィールドの説明

フィールド	説明
Entries	ND キャッシュの ND ネイバー エントリの総数。
High-Water	ND キャッシュの ND ネイバー エントリの最大数（現時点）。
Gleaned	グリーニングされた（つまり、ネイバー NA または他の ND パケットから学習した）ND ネイバー エントリの数。

フィールド	説明
Scavenged	タイムアウトになってキャッシュから削除された古い ND ネイバーの数。
Entry States	各状態の ND ネイバーの数。
Resolutions (INCMP)	INCMP 状態で試行された（つまり、データ パケットによって発生した）ネイバー解決の統計情報。 INCMP状態で試行された解決の詳細は、次のとおりです。 • Requested：要求された解決の総数。 • Timeouts：解決中に発生したタイムアウト回数。 • Resolved：成功した解決の数。 • Failed：成功しなかった解決の数。 • In-progress：処理中の解決の数。 • High-water：処理中の解決の最大数（現時点）。 • Throttled：処理中の解決の最大数の制限によって解決要求が無視された回数。 • Data discards：ネイバー解決を待機しているデータ パケットが破棄された数。
Resolutions (PROBE)	PROBE 状態で試行されたネイバー解決（つまり、データパケットによって発生した既存エントリの再解決）の統計情報。 • Requested：要求された解決の総数。 • Timeouts：解決中に発生したタイムアウト回数。 • Resolved：成功した解決の数。 • Failed：成功しなかった解決の数。

show ipv6 protocols

アクティブなIPv6ルーティングプロトコルプロセスのパラメータと現在の状態を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 protocols** コマンドを使用します。

show ipv6 protocols [summary]

構文の説明

summary	（任意）設定されたルーティング プロトコル プロセスの名前を表示します。

コマンド モード

ユーザ EXEC（>）

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(8)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.4(15)T	このコマンドが変更されました。 コマンド出力が、ベクトル メトリックを含む Enhanced Interior Gateway Routing Protocol（EIGRP）の情報を提供するように拡張されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.4	このコマンドが、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータに実装されました。

リリース	変更内容
Cisco IOS XE Release 3.6	このコマンドが変更されました。 コマンド出力が、EIGRP IPv6 Nonstop Forwarding（NSF）に関する情報を含むように拡張されました。
15.2(2)S	このコマンドが変更されました。 コマンド出力が、EIGRP IPv6 NSF に関する情報を含むように拡張されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

show ipv6 protocols コマンドにより表示される情報は、ルーティング操作のデバッグに役立ちます。

例

show ipv6 protocols コマンドの次の出力例は、Intermediate System-to-Intermediate System（IS-IS）ルーティング プロトコルの情報を示しています。

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"
  Interfaces:
    Ethernet0/0/3
    Ethernet0/0/1
    Serial1/0/1
    Loopback1 (Passive)
    Loopback2 (Passive)
    Loopback3 (Passive)
    Loopback4 (Passive)
    Loopback5 (Passive)
  Redistribution:
    Redistributing protocol static at level 1
  Inter-area redistribution
    Redistributing L1 into L2 using prefix-list word
  Address Summarization:
    L2: 33::/16  advertised with metric 0
    L2: 44::/16  advertised with metric 20
    L2: 66::/16  advertised with metric 10
    L2: 77::/16  advertised with metric 10
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *9*：*IS-IS* プロセスの *show ipv6 protocols* のフィールドの説明

フィールド	説明
IPv6 Routing Protocol is	使用される IPv6 ルーティング プロトコルを指定します。
Interfaces	IPv6 IS-IS プロトコルを設定するインターフェイスを指定します。

フィールド	説明
Redistribution	再配布されるプロトコルを示します。
Inter-area redistribution	他のレベルに再配布される IS-IS レベルを示します。
using prefix-list	エリア間再配布で使用されるプレフィックス リストに名前を付けます。
Address Summarization	すべてのサマリープレフィックスを示します。サマリー プレフィックスをアドバタイズすると、プレフィックスの後に「advertised with metric *x*」と表示されます。

show ipv6 protocols コマンドの次の出力例では、自律システム 30 のボーダー ゲートウェイ プロトコル（BGP）の情報が表示されます。

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "bgp 30"
  IGP synchronization is disabled
  Redistribution:
    Redistributing protocol connected
  Neighbor(s):
    Address                    FiltIn FiltOut Weight RoutemapIn RoutemapOut
    2001:DB8:0:ABCD::1            5       7    200
    2001:DB8:0:ABCD::2                                rmap-in    rmap-out
    2001:DB8:0:ABCD::3                                rmap-in    rmap-out
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *10*：*BGP* プロセスの *show ipv6 protocols* のフィールドの説明

フィールド	説明
IPv6 Routing Protocol is	使用される IPv6 ルーティング プロトコルを指定します。
Redistribution	再配布されるプロトコルを示します。
Address	ネイバーの IPv6 アドレス。
FiltIn	入力に適用される AS パス フィルタ リスト。
FiltOut	出力に適用される AS パス フィルタ リスト。
Weight	BGP 最良パス選択に使用するネイバーの重み値。

フィールド	説明
RoutemapIn	入力に適用されるネイバー ルート マップ。
RoutemapOut	出力に適用されるネイバー ルート マップ。

show ipv6 protocols summary コマンドの出力例を示します。

```
Device# show ipv6 protocols summary

Index Process Name
0     connected
1     static
2     rip myrip
3     bgp 30
```

show ipv6 protocols コマンドの次の出力例は、ベクトル メトリックおよびEIGRP IPv6 NSF を含むEIGRP 情報を表示しています。

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "bgp 1"
  IGP synchronization is disabled
  Redistribution:
    None
IPv6 Routing Protocol is "bgp multicast"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "eigrp 1"
EIGRP-IPv6 VR(name) Address-Family Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0 K6=0
  Metric rib-scale 128
  Metric version 64bit
  NSF-aware route hold timer is 260
  EIGRP NSF enabled
     NSF signal timer is 15s
     NSF converge timer is 65s
  Router-ID: 10.1.2.2
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 16
    Maximum hopcount 100
    Maximum metric variance 1
    Total Prefix Count: 0
    Total Redist Count: 0

  Interfaces:
  Redistribution:
    None
```

次に、Open Shortest Path First（OSPF）ドメインで再配布を設定した後、IPv6 プロトコル情報を表示する例を示します。

```
Device# redistribute ospf 1 match internal
Device(config-rtr)# end
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip 1"
  Interfaces:
    Ethernet0/1
    Loopback9
  Redistribution:
    Redistributing protocol ospf 1 (internal)
```

```
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0):
    Ethernet0/0
  Redistribution:
    None
```

show ipv6 route

IPv6 ルーティング テーブルの内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 route** コマンドを使用します。

show ipv6 route [*ipv6-address*| *ipv6-prefix*/*prefix-length* [**longer-prefixes**]| [*protocol*] | [**repair**] | [**updated** [**boot-up**] [*day month*] [*time*]]| **interface** *type number*| **nd**| **nsf**| **table** *table-id* | **watch**]

構文の説明

ipv6-address	（任意）特定の IPv6 アドレスのルーティング情報を表示します。
ipv6-prefix	（任意）特定の IPv6 ネットワークのルーティング情報を表示します。
/*prefix-length*	（任意）IPv6 プレフィックスの長さ。 プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す10進値です。 10 進数値の前にスラッシュ記号が必要です。
longer-prefixes	（任意）より長いプレフィックスエントリの出力を表示します。
protocol	（任意）ルーティング プロトコルの名前、またはキーワード **connected**、**local**、**mobile**、または **static**。 ルーティング プロトコルを指定する場合は、**bgp**、**isis**、**eigrp**、**ospf**、または **rip** のキーワードのいずれかを使用します。
repair	（任意）ルートと修復パスを表示します。
updated	（任意）ルートとタイムスタンプを表示します。
boot-up	（任意）起動時以降のルーティング情報を表示します。
day month	（任意）指定した月と日以降のルートを表示します。
time	（任意）*hh:mm* 形式で指定された時刻以降のルートを表示します。

interface	（任意）インターフェイスに関する情報を表示します。
type	（任意）インターフェイス タイプ。
number	（任意）インターフェイス番号。
nd	（任意）ネイバー探索（ND）が所有する IPv6 ルーティング情報ベース（RIB）からのルートだけが表示されます。
nsf	（任意）ノンストップ フォワーディング（NSF）状態のルートを表示します。
repair	（任意）
table *table-id*	（任意）指定されたテーブル ID の IPv6 RIB テーブル情報を表示します。 テーブル ID は 16 進表記である必要があります。 範囲は 0 ～ 0-0xFFFFFFFF です。
watch	（任意）ルート ウォッチャに関する情報を表示します。

コマンド デフォルト

オプションの構文要素のいずれも選択しない場合、すべてのアクティブなルーティング テーブルの、すべての IPv6 ルーティング情報が表示されます。

コマンド モード

ユーザ EXEC（>）

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.2(8)T	このコマンドが変更されました。 **isis** キーワードが追加され、I1 - ISIS L1、I2 - ISIS L2、および IA - IS-IS エリア間のフィールドがコマンドの出力に含まれました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。

リリース	変更内容
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。 タイマー情報が削除され、IPv6 マルチプロトコル ラベル スイッチング（MPLS）インターフェイスを表示するインジケータが追加されました。
12.2(13)T	このコマンドが変更されました。 タイマー情報が削除され、IPv6 MPLS インターフェイスを表示するインジケータが追加されました。
12.2(14)S	このコマンドが変更されました。 **longer-prefixes** キーワードが追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータに実装されました。
12.4(24)T	このコマンドは、Cisco IOS Release 12.4(24)T よりも前のリリースで変更されました。 **table**、**nsf**、**watch**、および **updated** キーワードと、*day*、*month*、*table-id*、および *time* 引数が追加されました。
15.2(2)S	このコマンドが変更されました。 コマンド出力が、ドット付き 10 進数形式のルート タグ値を含むように拡張されました。
Cisco IOS XE Release 3.6S	このコマンドが変更されました。 コマンド出力が、ドット付き 10 進数形式のルート タグ値を含むように拡張されました。
15.1(1)SY	**nd** キーワードが追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

IPv6 専用の情報である点を除いて、**show ipv6 route** コマンドの出力は、**show ip route** コマンドと類似しています。

ipv6-address 引数または *ipv6-prefix*/*prefix-length* 引数が指定されている場合、最長一致検索がルーティング テーブルから実行され、そのアドレスまたはネットワークのルート情報だけが表示されます。ルーティング プロトコルが指定されている場合、そのプロトコルのルートだけが表示されます。 **connected**、**local**、**mobile**、または **static** キーワードを指定した場合は、指定したルート タ

イプだけが表示されます。 **interface** キーワードと *type* および *number* 引数が指定されている場合、指定インターフェイスに固有のルートだけが表示されます。

例

次に、キーワードまたは引数が指定されていない場合の **show ipv6 route** コマンドの出力例を示します。

```
Device# show ipv6 route

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - IIS interarea
B   2001:DB8:4::2/48 [20/0]
     via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
L   2001:DB8:4::3/48 [0/0]
     via ::, Ethernet1/0
C   2001:DB8:4::4/48 [0/0]
     via ::, Ethernet1/0
LC  2001:DB8:4::5/48 [0/0]
     via ::, Loopback0
L   2001:DB8:4::6/48 [0/0]
     via ::, Serial6/0
C   2001:DB8:4::7/48 [0/0]
     via ::, Serial6/0
S   2001:DB8:4::8/48 [1/0]
     via 2001:DB8:1::1, Null
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *11*：*show ipv6 route* のフィールドの説明

フィールド	説明
Codes:	ルートを生成したプロトコルを示します。 表示される値は次のとおりです。 • B：BGP 生成 • C：接続済み • I1：ISIS L1：統合 IS-IS Level 1 生成 • I2：ISIS L2：統合 IS-IS Level 2 生成 • IA：ISIS エリア間：統合 IS-IS エリア間生成 • L：ローカル • R：RIP 生成 • S：スタティック
2001:DB8:4::2/48	リモート ネットワークの IPv6 プレフィックスを示します。

フィールド	説明
[20/0]	角カッコ内の最初の数字は、情報の発信元からのアドミニストレーティブディスタンスです。2 番めの数字はルートのメトリックです。
via FE80::A8BB:CCFF:FE02:8B00	リモートネットワークまでの次のデバイスのアドレスを指定します。

ipv6-address 引数または *ipv6-prefix*/*prefix-length* 引数が指定されている場合は、そのアドレスまたはネットワークのルート情報だけが表示されます。 次に、IPv6 プレフィックス 2001:DB8::/35 が指定されている場合の **show ipv6 route** コマンドの出力例を示します。 出力のフィールドは字句どおりです。

```
Device# show ipv6 route 2001:DB8::/35

IPv6 Routing Table - 261 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B 2001:DB8::/35 [20/3]
  via FE80::60:5C59:9E00:16, Tunnel1
```

プロトコルを指定する場合、その特定のルーティング プロトコルのルートだけが表示されます。次に、**show ipv6 route bgp** コマンドの出力例を示します。 出力のフィールドは字句どおりです。

```
Device# show ipv6 route bgp

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B   2001:DB8:4::4/64 [20/0]
     via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
```

次に、**show ipv6 route local** コマンドの出力例を示します。 出力のフィールドは字句どおりです。

```
Device# show ipv6 route local

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
L   2001:DB8:4::2/128 [0/0]
     via ::, Ethernet1/0
LC  2001:DB8:4::1/128 [0/0]
     via ::, Loopback0
L   2001:DB8:4::3/128 [0/0]
     via ::, Serial6/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

次に、6PE マルチパス機能がイネーブルの場合の **show ipv6 route** コマンドの出力例を示します。出力のフィールドは字句どおりです。

```
Device# show ipv6 route

IPv6 Routing Table - default - 19 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
```

```
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
.
.
.
B   2001:DB8::/64 [200/0]
     via ::FFFF:172.11.11.1
     via ::FFFF:172.30.30.1
```

関連コマンド

コマンド	説明
ipv6 route	スタティック IPv6 ルートを確立します。
show ipv6 interface	IPv6 インターフェイス情報を表示します。
show ipv6 route summary	IPv6 ルーティング テーブルの現在の内容をサマリー形式で表示します。
show ipv6 tunnel	IPv6 トンネル情報を表示します。

show ipv6 snooping capture-policy

メッセージ キャプチャのポリシーを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 snooping capture-policy** コマンドを使用します。

show ipv6 snooping capture-policy [**interface** *type number*]

構文の説明

interface *type number*	（任意）指定したインターフェイス タイプおよび番号の第 1 ホップ メッセージ タイプを表示します。

コマンド モード

ユーザ EXEC（>）

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

show ipv6 snooping capture-policy コマンドは、IPv6 第 1 ホップ メッセージ キャプチャ ポリシーを表示します。

例

次の例は、IPv6 ネイバー探索プロトコル（NDP）インスペクション機能およびルータ アドバタイズメント（RA）ガード機能が設定されているイーサネット 0/0 インターフェイスでの **show ipv6 snooping capture-policy** コマンド出力を示しています。

```
Router# show ipv6 snooping capture-policy

Hardware policy registered on Et0/0
Protocol  Protocol value  Message  Value  Action  Feature
ICMP      58              RS       85     punt    RA Guard
```

```
                                                 punt    ND Inspection
ICMP      58              RA        86           drop    RA guard
                                                 punt    ND Inspection
ICMP      58              NS        87           punt    ND Inspection
ICMP      58              NA        88           punt    ND Inspection
ICMP      58              REDIR     89           drop    RA Guard
                                                 punt    ND Inspection
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *12*：*show ipv6 snooping capture-policy* のフィールドの説明

フィールド	説明
Hardware policy registered on Fa4/11	ハードウェア ポリシーには、プログラマティック アクセス リスト（ACL）とアクセス コントロール エントリ（ACE）が含まれています。
Protocol	パケットが検査されるプロトコル。
Message	検査するメッセージのタイプ。
Action	パケットで実行するアクション。
Feature	この情報用のインスペクション機能。

show ipv6 snooping counters

インターフェイス カウンタによってカウントされたパケットに関する情報を表示するには、ユーザ EXEC または特権 EXEC モードで **show ipv6 snooping counters** コマンドを使用します。

show ipv6 snooping counters [**interface** *type number*]

構文の説明

interface *type number*	（任意）指定したインターフェイス タイプおよび番号と一致する第1ホップ パケットを表示します。

コマンド モード

ユーザ EXEC、特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

show ipv6 snooping counters コマンドは、インターフェイス カウンタでカウントされている、スイッチャーによって処理されたパケットを表示します。 スイッチャーはインターフェイスごとにキャプチャされたパケットをカウントし、パケットが受信されたか、送信されたか、ドロップされたかを記録します。 パケットがドロップされた場合、ドロップの理由とドロップの原因となった機能の両方が記載されます。

例

次に、インターフェイス FastEthernet4/12 でカウントされたパケットに関する情報を表示する例を示します。

```
Router# show ipv6 snooping counters interface Fa4/12
Received messages on Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
```

```
                0       4256    0       0       0       0       0
Bridged messages from Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
                0       4240    0       0       0       0       0
Dropped messages on Fa4/12:
Feature/Message RS      RA      NS      NA      REDIR   CPS     CPA
RA guard        0       16      0       0       0       0       0
Dropped reasons on Fa4/12:
RA guard         16   RA drop - reason:RA/REDIR received on un-authorized port
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *13*：*show ipv6 snooping counters* のフィールドの説明

フィールド	説明
Received messages on Fa4/12:	インターフェイスで受信されたメッセージ。
Protocol	メッセージがカウントされているプロトコル。
Protocol message	カウントされているプロトコルメッセージのタイプ。
Bridged messages from Fa4/12:	インターフェイスからブリッジされたメッセージ。
Dropped messages an Fa4/12:	インターフェイス上でドロップされたメッセージ。
Feature/message	ドロップの原因となった機能、およびドロップされたメッセージのタイプと数。
RA drop - reason:RA/REDIR received on un-authorized port	これらのメッセージがドロップされた理由。

show ipv6 snooping features

ルータに設定されているスヌーピング機能に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 snooping features** コマンドを使用します。

show ipv6 snooping features

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC（>）

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。

使用上のガイドライン

show ipv6 snooping features コマンドは、ルータに設定されている第 1 ホップ機能を表示します。

例

次に、IPv6 ND インスペクションと IPv6 RA ガードの両方がルータに設定されている例を示します。

```
Router# show ipv6 snooping features

Feature name   priority state
RA guard          100   READY
NDP inspection     20   READY
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *14* : ***show ipv6 snooping features*** のフィールドの説明

フィールド	説明
Feature name	ルータに設定されている IPv6 グローバル ポリシー機能の名前。

フィールド	説明
Priority	指定された機能のプライオリティ。
State	指定された機能のステータス。

show ipv6 snooping policies

設定したポリシーと、それが適用されたインターフェイスに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 snooping policies** コマンドを使用します。

show ipv6 snooping policies [**interface** *type number*]

構文の説明

interface *type number*	（任意）指定したインターフェイスタイプおよび番号に一致するポリシーを表示します。

コマンド モード

ユーザ EXEC（>）

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。

使用上のガイドライン

show ipv6 snooping policies コマンドは、設定されているすべてのポリシーと、それが適用されたインターフェイスを表示します。

例

次に、設定されているすべてのポリシーの情報を表示する例を示します。

```
Device# show ipv6 snooping policies

NDP inspection policies configured:
Policy      Interface    Vlan
------      ---------    ----
trusted      Et0/0        all
             Et1/0        all
untrusted    Et2/0        all
RA guard policies configured:
Policy      Interface    Vlan
------      ---------    ----
host         Et0/0        all
             Et1/0        all
router       Et2/0        all
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *15* : ***show ipv6 first-hop policies*** フィールドの説明

フィールド	説明
NDP inspection policies configured:	特定の機能用に設定されたポリシーの説明。
Policy	ポリシーが信頼できるか、信頼できないか。
Interface	ポリシーが適用されるインターフェイス。

show ipv6 traffic

IPv6 トラフィックの統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 traffic**コマンドを使用します。

show ipv6 traffic [**interface** [*interface type number*]]

構文の説明

interface	（任意）すべてのインターフェイス。 IPv6 転送の統計情報が保存されているすべてのインターフェイスの IPv6 転送の統計情報が表示されます。
interface type number	（任意）指定したインターフェイス。特定のインターフェイスで最後にクリアされてから発生したインターフェイス統計情報が表示されます。

コマンド モード

ユーザ EXEC 特権 EXEC

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合され、出力フィールドが追加されました。
12.2(13)T	出力フィールドを追加する変更がこのリリースに統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

リリース	変更内容
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.2(33)SRC	*interface* 引数および **interface** キーワードが追加されました。
12.2(33)SB	このコマンドが、Cisco IOS Release 12.2(33)SB に統合されました。
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ デバイスで追加されました。
15.2(2)SNG	このコマンドが、Cisco ASR 901 シリーズのアグリゲーション サービス デバイスに実装されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

show ipv6 traffic コマンドの出力は、IPv6 に固有である点を除き、**show ip traffic** コマンドの出力と似ています。

例

次に、**show ipv6 traffic** コマンドの出力例を示します。

```
Device# show ipv6 traffic
IPv6 statistics:
  Rcvd:  0 total, 0 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a device
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
         0 unicast RPF drop, 0 suppressed RPF drop
  Sent:  0 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent
ICMP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 device solicit, 0 device advert, 0 redirects
```

次に、IPv6 CEF を実行しない show ipv6 interface コマンドの出力例を示します。

```
Device# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFF:FE49:9
  Description: sat-2900a f0/12
```

```
  Global unicast address(es):
    7::7, subnet is 7::/32
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Input features: RPF
  Unicast RPF access-list MINI
    Process Switching:
      0 verification drops
      0 suppressed verification drops
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
```

次に、IPv6 CEF を実行している show ipv6 interface コマンドの出力例を示します。

```
Device# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFF:FE49:9
  Description: sat-2900a f0/12
  Global unicast address(es):
    7::7, subnet is 7::/32
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Input features: RPF
  Unicast RPF access-list MINI
    Process Switching:
      0 verification drops
      0 suppressed verification drops
    CEF Switching:
      0 verification drops
      0 suppressed verification drops
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *16*：*show ipv6 traffic* のフィールドの説明

フィールド	説明
source-routed	発信元からルーティングされたパケットの数。
truncated	切り捨てられたパケットの数。
format errors	ヘッダーフィールド、バージョン番号、パケット長で実行されたチェックの結果として生じた可能性があるエラー。

フィールド	説明
not a device	IPv6 ユニキャスト ルーティングがイネーブルになっていないときに送信されたメッセージ。
0 unicast RPF drop, 0 suppressed RPF drop	ユニキャスト リバース パス転送（RPF）および抑制された RPF のドロップ数。
failed	失敗したフラグメント送信の数。
encapsulation failed	未解決のアドレスまたはトライアンドキューパケットが原因と考えられる失敗。
no route	ソフトウェアが送信方法を認識していなかったデータグラムを廃棄するときにカウントされます。
unreach	受信される到達不能メッセージは次のとおりです。 • routing：宛先へのルートがないことを示します。 • admin：宛先との通信が管理上禁止されていることを示します。 • neighbor：宛先が送信元アドレスの範囲外であることを示します。 たとえば、送信元がローカル サイトであるか、宛先に送信元へ戻るルートがない可能性があります。 • address：アドレスが到達不能であることを示します。 • port：ポートが到達不能であることを示します。
Unicast RPF access-list MINI	使用中のユニキャスト RPF アクセスリスト。
Process Switching	検証や抑制された検証のドロップなど、プロセス RPF の数を表示します。
CEF Switching	検証のドロップや抑制された検証のドロップなど、CEF スイッチングの数を表示します。

summary-prefix（OSPFv3）

Open Shortest Path First バージョン 3（OSPFv3）の IPv6 サマリー プレフィックスを設定するには、OSPFv3 ルータ コンフィギュレーション モード、IPv6 アドレス ファミリ コンフィギュレーション モード、または IPv4 アドレス ファミリ コンフィギュレーション モードで **summary-prefix** コマンドを使用します。 デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

summary-prefix *prefix* [**not-advertise**| **tag** *tag-value*] [**nssa-only**]

no summary-prefix *prefix* [**not-advertise**| **tag** *tag-value*] [**nssa-only**]

構文の説明

prefix	宛先の IPv6 ルート プレフィックス。
not-advertise	（任意）指定されたプレフィックス/マスク ペアと一致するルートを抑制します。 このキーワードは OSPFv3 だけに適用されます。
tag *tag-value*	（任意）ルートマップを使用して再配布を制御する match 値として使用できるタグ値を指定します。 このキーワードは OSPFv3 だけに適用されます。
nssa-only	（任意）プレフィックスの範囲をエリアに限定します。 指定したプレフィックスに対して生成されるサマリー ルート（存在する場合）に nssa-only 属性を設定します。

コマンド デフォルト

IPv6 サマリー プレフィックスは定義されていません。

コマンド モード

OSPFv3 ルータ コンフィギュレーション モード（config-router）

IPv6 アドレス ファミリ コンフィギュレーション（config-router-af）

IPv4 アドレス ファミリ コンフィギュレーション（config-router-af）

コマンド履歴

リリース	変更内容
12.0(24)S	このコマンドが導入されました。
12.2(15)T	このコマンドが、Cisco IOS Release 12.2(15)T に統合されました。

リリース	変更内容
12.2(18)S	このコマンドが、Cisco IOS Release 12.2(18)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
15.1(3)S	このコマンドが変更されました。 コマンドは IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
Cisco IOS XE Release 3.4S	このコマンドが変更されました。 コマンドは IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
15.2(1)T	このコマンドが変更されました。 コマンドは IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
15.2(4)S	このコマンドが変更されました。 キーワード **nssa-only** が追加されました。
15.1(1)SY	このコマンドが変更されました。 コマンドは IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

summary-prefix コマンドは、別のルーティング プロトコルから再配布されたデバイスを集約するために使用できます。 複数のアドレス グループを集約できます。 サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。 このコマンドは、ルーティング テーブルの容量縮小に有効です。

外部ルートが Not So Stubby Area（NSSA）に再配布される場合、Propagate ビット（P ビット）をクリアするために **nssa-only** キーワードを指定します。 これにより、対応する NSSA 外部リンク ステート アドバタイズメント（LSA）が他のエリアに変換されることを防ぎます。

例

次の例で、サマリープレフィックス 2051:0:0:10::/60 には 2051:0:0:10::/60 から 2051:0:0:20::/128（ただし、このアドレスは含まれない）までのアドレスが含まれます。 アドレス 2051:0:0:10::/60 だけが外部 LSA でアドバタイズされます。

```
summary-prefix 2051:0:0:10::/60
```

関連コマンド

router ospfv3	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。

throttle-period

IPv6 ルータ アドバタイズメント（RA）スロットル ポリシーのスロットル期間を設定するには、IPv6 RA スロットル ポリシー コンフィギュレーション モードで **throttle-period** コマンドを使用します。 このコマンドをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

throttle-period { **inherit**| *seconds*}

構文の説明

inherit	スロットル期間の設定はターゲット ポリシーから継承されます。
seconds	スロットル期間の時間（秒単位）。 範囲は 10 ～ 86,400 秒です。

コマンド デフォルト

600 秒（10 分）

コマンド モード

IPv6 RA スロットル ポリシー コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

throttle-period コマンドは、VLAN に適用されたポリシーにのみ有効です。 ポートでこのコマンドを設定しようとすると、ポートはこれを無視します。

例

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# throttle-period 300
```

timers spf（IPv6）

IPv6 の Open Shortest Path First（OSPF）の Shortest Path First（SPF）スロットリングをオンにするには、ルータ コンフィギュレーション モードで **timers spf** コマンドを使用します。 SPF スロットリングをオフにするには、このコマンドの **no** 形式を使用します。

timers spf *delay holdtime*

no timers spf

構文の説明

delay	SPF 計算の変更を受信する遅延（ミリ秒）。 指定できる範囲は 0 ～ 4294967295 です。 デフォルトは 5 ミリ秒です。
holdtime	連続する SPF 計算間のホールド時間（ミリ秒単位）。 指定できる範囲は 0 ～ 4294967295 です。 デフォルトは 10 ミリ秒です。

コマンド デフォルト

OSPF for IPv6 スロットリングは常にイネーブルです。

コマンド モード

ルータ コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(15)T	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

SPF 計算間の初回待機時間は、*delay* 引数で指定される時間（ミリ秒）です。 続いて適用される各待機時間は、待機時間が *holdtime* 引数で指定される最大時間（ミリ秒）に達するまで、現在の保持時間（ミリ秒）を 2 倍した値になります。 値がリセットされるまで、または SPF 計算間でリンクステートアドバタイズメント（LSA）が受信されるまで、従属待機時間は最大のまま残ります。

例

次に、**timers spf** コマンドの遅延時間とホールド時間の間隔値をそれぞれ 40 ミリ秒と 50 ミリ秒に設定したルータの例を示します。

```
Router(config)# ipv6 router ospf 1
Router(config-router)# timers spf 40 50
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPF for IPv6 ルーティング プロセスに関する一般情報を表示します。

timers throttle lsa

IPv6 の Open Shortest Path First（OSPF）のリンクステート アドバタイズメント（LSA）の生成に関するレート制限値を設定するには、ルータ コンフィギュレーション モードで **timers throttle lsa** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

timers throttle lsa *start-interval hold-interval max-interval*

no timers throttle lsa

構文の説明

start-interval	LSA の生成の最小遅延（ミリ秒単位）。 LSA の最初のインスタンスは、ローカル OSPF for IPv6 トポロジの変更の直後に必ず生成されます。 次の LSA の生成は、開始間隔の前ではありません。 範囲は 0 ～ 600,000 ミリ秒です。 デフォルト値は 0 ミリ秒です。つまり、遅延はなく、LSA は即座に送信されます。
hold-interval	増分時間（ミリ秒単位）。 この値は、LSA 生成の時間を制限する従属レートを計算するために使用されます。 範囲は 1 ～ 600,000 ミリ秒です。 デフォルト値は 5000 ミリ秒です。
max-interval	同じ LSA の生成間の最大待機時間（ミリ秒単位）。 範囲は 1 ～ 600,000 ミリ秒です。 デフォルト値は 5000 ミリ秒です。

コマンド デフォルト

start-interval：0 ミリ秒*hold-interval*：5000 ミリ秒*max-interval*：5000 ミリ秒

コマンド モード

OSPF for IPv6 ルータ コンフィギュレーション（config-rtr）ルータ コンフィギュレーション（config-router）

コマンド履歴

リリース	変更内容
12.2(33)SRC	このコマンドが導入されました。
12.2(33)SB	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ ルータで追加されました。
15.0(1)M	このコマンドが、Cisco IOS Release 12.5(1)M に統合されました。
12.2(33)XNE	このコマンドが変更されました。 Cisco IOS Release 12.2(33)XNE に統合されました。
15.1(1)SY	このコマンドが変更されました。 Cisco IOS Release 15.1(1)SY に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

「同じ LSA」とは、同じ LSA ID 番号、LSA タイプ、およびアドバタイズ ルータ ID を含む LSA インスタンスを意味します。 **timers lsa arrival** コマンドの *milliseconds* 値は、**timers throttle lsa** コマンドの *hold-interval* 値以下にすることをお勧めします。

例

この例では、OSPF LSA スロットリングをカスタマイズして、開始間隔が 200 ミリ秒、ホールド間隔が 10,000 ミリ秒、最大間隔が 45,000 ミリ秒になるようにしています。 同じ LSA を受信するインスタンス間の最小間隔は 2000 ミリ秒です。

```
router ospf 1
 log-adjacency-changes
 timers throttle lsa 200 10000 45000
 timers lsa arrival 2000
 network 10.10.4.0 0.0.0.255 area 24
 network 10.10.24.0 0.0.0.255 area 24
```

この例では、IPv6 OSPF LSA スロットリングをカスタマイズして、開始間隔が 500 ミリ秒、ホールド間隔が 1,000 ミリ秒、最大間隔が 10,000 ミリ秒になるようにしています。

```
ipv6 router ospf 1
 log-adjacency-changes
 timers throttle lsa 500 1000 10000
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPF for IPv6 ルーティング プロセスに関する情報を表示します。
timers lsa arrival	ソフトウェアが OSPF ネイバーから同一の LSA を受け入れる最小間隔を設定します。

tracking

ポートのデフォルト トラッキング ポリシーを上書きするには、ネイバー探索（ND）インスペクション ポリシー コンフィギュレーション モードで **tracking** コマンドを使用します。

tracking {**enable** [**reachable-lifetime** {*value*| **infinite**}]| **disable** [**stale-lifetime** {*value*| **infinite**}]}

構文の説明

enable	トラッキングはイネーブルです。
reachable-lifetime	（任意）到達可能なエントリが、到達可能性の確認なしで直接的または間接的に到達可能であると見なされる時間の上限。 • **reachable-lifetime** キーワードは、**enable** キーワードとのみ使用可能です。 • **reachable-lifetime** キーワードは、**ipv6 neighbor binding reachable-lifetime** コマンドで設定されたグローバルな到達可能ライフタイムよりも優先されます。
value	秒単位のライフタイム値。 指定できる範囲は 1 ～ 86400 で、デフォルトは 300 です。
infinite	到達可能状態または STALE 状態のエントリを時間制限なしに保持します。
disable	トラッキングをディセーブルにします。
stale-lifetime	（任意）STALE状態のエントリを保持する時間で、グローバルな stale-lifetime 設定を上書きします。 • STALE ライフタイムは 86,400 秒です。 • **stale-lifetime** キーワードは、**enable** キーワードとのみ使用可能です。 • **stale-lifetime** キーワードは、**ipv6 neighbor binding stale-lifetime** コマンドで設定されたグローバルな STALE ライフタイムよりも優先されます。

コマンド モード

ND エントリが到達可能状態で保持される時間。ュレーション（config-nd-inspection）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。

使用上のガイドライン

tracking コマンドは、このポリシーが適用されるポートで **ipv6 neighbor tracking** コマンドによって設定されたデフォルトのトラッキングポリシーを上書きします。この機能は、たとえば、エントリを追跡したくはないが、エントリがなくならないようにバインディング テーブル内に保持したいような、信頼できるポートで便利です。

reachable-lifetime キーワードは、追跡による直接的な、または ND インスペクションによる間接的な到達可能性の確認なしで、エントリが到達可能と見なされる最大時間です。 **reachable-lifetime** 値に到達すると、エントリは STALE に移動されます。 **tracking** コマンドの **reachable-lifetime** キーワードは、**ipv6 neighbor binding reachable-lifetime** コマンドで設定されたグローバルな到達可能ライフタイムよりも優先されます。

stale-lifetime キーワードは、エントリが削除されるか、エントリに到達可能であることが直接または間接的に確認される前に、エントリをテーブルに保持する最大時間です。 **tracking** コマンドの **stale-lifetime** キーワードは、**ipv6 neighbor binding stale-lifetime** コマンドで設定されたグローバルな STALE ライフタイムよりも優先されます。

例

次の例では、policy1 として ND ポリシー名を定義し、ルータを ND インスペクション ポリシー コンフィギュレーション モードにして、信頼できるポートで時間制限なしにエントリがバインディング テーブルに留まるように設定します。

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# tracking disable stale-lifetime infinite
```

関連コマンド

コマンド	説明
ipv6 nd inspection policy	ND インスペクション ポリシー名を定義して、ND インスペクション ポリシー コンフィギュレーション モードを開始します。
ipv6 neighbor binding	バインディング テーブルのネイバー バインディング エントリのデフォルトを変更します。

コマンド	説明
ipv6 neighbor tracking	バインディングテーブルのエントリのトラッキングをイネーブルにします。
ipv6 nd raguard policy	RA ガード ポリシー名を定義し、RA ガード ポリシー コンフィギュレーション モードを開始します。

tunnel mode ipv6ip

スタティック IPv6 トンネル インターフェイスを設定するには、インターフェイス コンフィギュレーション モードで **tunnel mode ipv6ip** コマンドを使用します。 スタティック IPv6 トンネル インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

tunnel mode ipv6ip [**6rd**| **6to4**| **auto-tunnel**| **isatap**]

no tunnel mode ipv6ip

構文の説明

6rd	（任意）トンネルが IPv6 Rapid Deployment（6RD）を使用するように指定します。
6to4	（任意）IPv4 アドレスとプレフィックス 2002::/16 から動的に生成された宛先アドレス（6to4 アドレスと呼ばれます）を使用して IPv6 自動トンネルを設定します。
auto-tunnel	（任意）IPv4 互換 IPv6 アドレスを使用して IPv6 自動トンネルを設定します。
isatap	（任意）Intra-Site Automatic Tunnel Addressing Protocol（ISATAP）を使用して IPv4 ネットワーク内の IPv6 ノード（ホストとルータ）に接続する IPv6 自動トンネルを設定します。

コマンド デフォルト

スタティック IPv6 トンネル インターフェイスは設定されていません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。

リリース	変更内容
12.2(14)S	このコマンドが変更されました。 **isatap** キーワードが、ISATAP トンネルの実装の追加をサポートするために追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。
Cisco IOS XE Release 3.1S	このコマンドが変更されました。 **6rd** キーワードが追加されました。 **auto-tunnel** キーワードが、Cisco ASR 1000 シリーズ ルータで廃止されました。
15.1(3)T	このコマンドが Cisco IOS Release 15.1(3)T に統合されました。
15.1SY	このコマンドが Cisco IOS Release 15.1SY に統合されました。 **auto-tunnel** キーワードが廃止されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

IPv6 トンネリングとは、IPv4 パケットに IPv6 パケットをカプセル化し、IPv4 ルーティング インフラストラクチャを介してパケットを送信することです。

手動設定トンネル

tunnel mode ipv6ip コマンドは IPv6 トンネルを設定します。 IPv6 トンネルの両端のデバイスは、IPv4 と IPv6 の両方のプロトコル スタックをサポートする必要があります。

このコマンドを使用するには、まず手動で以下を設定する必要があります。

- トンネル インターフェイスの IPv6 アドレス
- トンネルの送信元として IPv4 アドレス
- トンネルの宛先として IPv4 アドレス

トンネルの宛先の自動判別

tunnel mode ipv6ip auto-tunnel コマンドは自動 IPv6 トンネルを設定します。 トンネル送信元は手動で設定します。 トンネル宛先は、IPv4 互換 IPv6 アドレスの下位 32 ビットとして自動的に定められます。 IPv4 互換 IPv6 アドレスは、アドレスの上位 96 ビットに IPv6 プレフィックス 0:0:0:0:0:0 を含み、アドレスの下位 32 ビットに IPv4 アドレスを含む 128 ビットの IPv6 アドレスです。 自動

トンネルの両端のデバイスは、IPv4 と IPv6 の両方のプロトコル スタックをサポートする必要があります。

6to4 トンネル

tunnel mode ipv6ip 6to4 コマンドは、グローバルに一意な IPv4 アドレスを 6to4 アドレスに埋め込むことでトンネル エンドポイントが決定される自動 6to4 トンネルを設定します。 6to4 アドレスは、プレフィックス 2002::/16 とグローバルに一意な 32 ビットの IPv4 アドレスの組み合わせです。（IPv4 互換アドレスは、6to4 トンネリングでは使用されません）。一意な IPv4 アドレスが、6to4 アドレス プレフィックスで、ネットワーク層アドレスとして使用されます。 トンネルの送信元は、**tunnel source** コマンドを使用して手動で設定できるインターフェイスです。 6to4 トンネルの両端の境界デバイスは、IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。 さらに、6to4 アドレス プレフィックスでネットワークに宛先指定されたトラフィックは、**ipv6 route** コマンドを使用して、トンネルを介してルーティングされる必要があります。

6RD トンネル

tunnel mode ipv6ip 6rd コマンドは、トンネルが IPv6 RD 用に使用されることを指定します。 6RD 機能は、6to4 トンネル機能に似ていますが、アドレスに 2002::/16 プレフィックスは必要ありません。 IPv4 宛先の 32 ビットがすべて IPv6 ペイロード ヘッダーにあることも必要としません。

ISATAP トンネル

ISATAP トンネルはネットワーク境界内での IPv6 パケットの転送をイネーブルにします。 ISATAP トンネルによって、サイト内の IPv4 または IPv6 デュアル スタック ホストが個別に IPv4 インフラストラクチャを使用して IPv6 ネットワークに接続できます。

IPv4 互換アドレスとは異なり、ISATAP IPv6 アドレスは任意のユニキャスト /64 の最初のプレフィックスを使用できます。 最後の 64 ビットは、インターフェイス ID として使用されます。 これらの、最初の 32 ビットは固定パターンの 0000:5EFE です。 最後の 32 ビットには、トンネル エンドポイントの IPv4 アドレスが含まれます。

例

例

次に、手動で IPv6 トンネルを設定する例を示します。 この例では、トンネル インターフェイス 0 が、グローバル IPv6 アドレスを使用して手動で設定されます。 トンネル送信元およびトンネル宛先も、手動で設定されます。

```
Device(config)# interface tunnel 0
Device(config-if)# ipv6 address 3ffe:b00:c18:1::3/127
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel destination 192.168.30.1
Device(config-if)# tunnel mode ipv6ip
Device(config-if)# end
```

例

次に、トンネル送信元として、イーサネットインターフェイス0を使用する自動IPv6トンネルを設定する例を示します。 トンネル宛先は、IPv4互換IPv6アドレスの下位32ビットとして自動的に定められます。

```
Device(config)# interface tunnel 0
Device(config-if)# no ip address
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel mode ipv6ip auto-tunnel
Device(config-if)# end
```

例

次に、6to4トンネルを設定する例を示します。 この例では、イーサネットインターフェイス0がIPv4アドレス192.168.99.1によって設定されます。 サイト固有の48ビットプレフィックス2002:c0a8:630が、プレフィックス2002::/16をIPv4アドレス192.168.99.1に追加することにより構築されます。

トンネルインターフェイス0は、IPv4またはIPv6アドレスなしで設定されます。 トンネル送信元アドレスは、イーサネットインターフェイス0として手動で設定されます。 トンネル宛先アドレスは自動的に構築されます。 IPv6スタティックルートは、ネットワーク2002::/16に宛先指定されたトラフィックをトンネルインターフェイス0でルーティングするように設定されます。

```
Device(config)# interface ethernet 0
Device(config-if)# ip address 192.168.99.1 255.255.255.0
Device(config-if)# ipv6 address 2002:c0a8:6301:1::/64 eui-64
Device(config-if)# exit
Device(config)# interface tunnel 0
Device(config-if)# no ip address
Device(config-if)# ipv6 unnumbered ethernet 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel mode ipv6ip 6to4
Device(config-if)# exit
Device(config)# ipv6 route 2002::/16 tunnel 0
Device(config)# end
```

例

ipv6 unnumbered、**tunnel source**、および**tunnel mode ipv6ip** コマンドを使用してトンネルインターフェイスが設定されている場合、トンネルは、IPv6アドレスとして送信元インターフェイスに設定されている最初のIPv6アドレスを使用します。 6to4トンネルの場合、送信元インターフェイスに設定される最初のIPv6アドレスは、6to4アドレスである必要があります。 次の例では、イーサネットインターフェイス0に最初に設定されるIPv6アドレス（6to4アドレス2002:c0a8:6301:1::/64）が、トンネル0のIPv6アドレスとして使用されます。

```
Device(config)# interface tunnel 0
Device(config-if)# ipv6 unnumbered ethernet 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel mode ipv6ip 6to4
Device(config-if)# exit
Device(config)# interface ethernet 0
Device(config-if)# ipv6 address 2002:c0a8:6301:1::/64 eui-64
Device(config-if)# ipv6 address 3ffe:1234:5678::1/64
Device(config-if)# end
```

例

次に、6RD トンネルを設定する例を示します。

```
Device(config)# interface Tunnel1
Device(config-if)# ipv6 address 2001:B000:100::1/32
Device(config-if)# tunnel source GigabitEthernet2/0/0
Device(config-if)# tunnel mode ipv6ip 6rd
Device(config-if)# tunnel 6rd prefix 2001:B000::/32
Device(config-if)# tunnel 6rd ipv4 prefix-len 16 suffix-len 8
Device(config-if)# end
Device# show tunnel 6rd Tunnel1

Interface Tunnel1:
  Tunnel Source: 10.1.1.1
  6RD: Operational, V6 Prefix: 2001:B000::/32
       V4 Common Prefix Length: 16, Value: 10.1.0.0
       V4 Common Suffix Length: 8, Value: 0.0.0.1
```

例

次に、イーサネット インターフェイス 0 に ISATAP トンネルを設定する例を示します。 クライアントの自動設定を可能にするために、ルータ アドバタイズメントがイネーブルになっています。

```
Device(config)# interface Ethernet 0
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config)# interface Tunnel 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel mode ipv6ip isatap
Device(config-if)# ipv6 address 2001:0DB8::/64 eui-64
Device(config-if)# no ipv6 nd ra suppress
Device(config-if)# end
```

関連コマンド

コマンド	説明
ip address	IPv4 インターフェイスの IP アドレスを指定します。
ipv6 address	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ipv6 address eui-64	インターフェイスの IPv6 アドレスを設定し、アドレスの下位 64 ビットの EUI-64 インターフェイス ID を使用してインターフェイスで IPv6 処理をイネーブルにします。
ipv6 route	スタティック IPv6 ルートを確立します。
ipv6 unnumbered	インターフェイスに明示的な IPv6 アドレスを割り当てなくても、インターフェイスで IPv6 処理をイネーブルにします。

コマンド	説明
no ipv6 nd ra suppress	LAN インターフェイスでの IPv6 ルータ アドバタイズメントの送信を再びイネーブルにします。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。
show tunnel 6rd tunnel	トンネルに関する 6RD 情報を表示します。
tunnel 6rd ipv4	ドメイン内のすべての 6RD ルータに共通の IPv4 トランスポートアドレスのプレフィックス長およびサフィクス長を指定します。
tunnel 6rd prefix	6RD トンネルで共通の IPv6 プレフィックスを指定します。
tunnel destination	トンネルインターフェイスの宛先アドレスを設定します。
tunnel source	トンネルインターフェイスの送信元アドレスを設定します。

vlan configuration

VLANまたはVLANのコレクションを設定し、VLANコンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **vlan configuration** コマンドを使用します。コマンドのデフォルトに戻すには、このコマンドの **no** 形式を使用します。

vlan configuration *vlan-id*

構文の説明

vlan-id	VLAN または VLAN のコレクション。

コマンド デフォルト

VLAN または VLAN のコレクションは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

VLAN または VLAN のコレクションを設定するには、**vlan configuration** コマンドを使用します。VLAN レベルで機能する IPv6 RA スロットルは、指定された時間、VLAN 上で複数のデバイスからのすべての RA をカウントします。

ipv6 nd ra-throttle policy コマンドを使用して IPv6 RA スロットル ポリシーを設定した後、**ipv6 nd ra-throttle attach-policy** コマンドを使用してVLANまたはVLANのコレクションに適用できます。

例

```
Device(config)# vlan configuration vlan1
Device(config-vlan-config)#
```